CONFIDENTIALITY COALITION

GENERAL COMMITTEE MEETING

Thursday, January 25, 2018
3:00 PM to 4:00 PM

Healthcare Leadership Council
750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 857-232-0157, 30-40-73#

1. Welcome and introductions

2. Speaker: Kathryn Marchesini, ONC chief privacy officer (*invited*)

3. Clearinghouse bill update

a. H.R. 4613	Attachment 1
b. H.R. 4613 Talking Points	Attachment 2
c. Clearinghouse Articles	Attachments 3,4,5,6

4. TEFCA Framework Attachment 7

5. Cybersecurity update

a. Cybersecurity side by side chart	Attachment 8
b. NH-ISAC Healthcare Sector Coordinating Council	Attachment 9
c. HPH SCC Cybersecurity Working Group PowerPoint	Attachment 10

I

115TH CONGRESS
1ST SESSION

H. R. 4613

To allow the use of claims, eligibility, and payment data to produce reports, analyses, and presentations to benefit Medicare, and other similar health insurance programs, entities, researchers, and health care providers, to help develop cost saving approaches, standards, and reference materials and to support medical care and improved payment models.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 11, 2017

Mrs. MCMORRIS RODGERS (for herself, Mr. KELLY of Pennsylvania, Mr. HUDSON, Mrs. BLACKBURN, Mr. LONG, Mr. BISHOP of Michigan, Mr. PAULSEN, and Mr. KRISHNAMOORTHI) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Ways and Means, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To allow the use of claims, eligibility, and payment data to produce reports, analyses, and presentations to benefit Medicare, and other similar health insurance programs, entities, researchers, and health care providers, to help develop cost saving approaches, standards, and reference materials and to support medical care and improved payment models.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Ensuring Patient Access to Healthcare Records Act of 2017".

SEC. 2. PROMOTION OF ACCESS TO DATA, VIA RESEARCH AND USER FRIENDLY PRESENTATIONS AND APPLICATIONS.

(a) IN GENERAL.—Subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.) is amended by adding at the end the following:

"PART 3—HEALTH CARE CLEARINGHOUSES; DATA PROCESSING TO EMPOWER PATIENTS AND IMPROVE THE HEALTH CARE SYSTEM

"SEC. 13451. MODERNIZING THE ROLE OF CLEARINGHOUSES IN HEALTH CARE.

"(a) EFFORTS TO PROMOTE ACCESS TO AND LEVERAGING OF HEALTH INFORMATION.—

"(1) IN GENERAL.—The Secretary shall, through the updating of existing policies and development of policies that support dynamic technology solutions, promote patient access to information related to their care, including real world outcomes and economic data (including claims, eligibility, and payment data), in a manner that would ensure that such information is available in a form convenient

for the patient, in a reasonable manner, and without burdening the health care provider involved.

"(2) REQUIREMENT.—Activities carried out under paragraph (1) shall include the development of policies to enable covered entities with access to health information to—

"(A) provide patient access to information related to their care, including real world outcomes and economic data;

"(B) develop, in accordance with HIPAA-related provisions (as defined in subsection (j)), patient engagement tools, reports, analyses, and presentations based on population health, epidemiological, and health services outcomes data, that may demonstrate a fiscal or treatment benefit to patients and health plan enrollees; and

"(C) promote transparency regarding the use and disclosure of health information by health care clearinghouses in accordance with the notice provisions of subsection (e).

"(b) TREATMENT AS COVERED ENTITY FOR SPECIFIED FUNCTIONS.—

"(1) IN GENERAL.—With respect to the use and disclosure of protected health information, the Secretary shall—

"(A) not consider health care clearinghouses that engage in the functions described in paragraph (3) to be business associates, including subcontractor business associates, under HIPAA-related provisions (as defined in subsection (j)(3)) regardless of the role of such clearinghouses in collecting or receiving the information; and

"(B) consider such clearinghouses to be covered entities under such provisions of law for all purposes.

Such clearinghouses shall not be considered business associates, or subcontractor business associates, for translation of data into and out of standard format, analytic, cloud computing, or any other purpose.

"(2) DATA ACCURACY AND SECURITY REQUIREMENT.—In order to use health data as authorized by this section, a clearinghouse or other covered entity engaging in activities authorized under this section shall be certified to have the necessary expertise and technical infrastructure to ensure the accuracy and security of such claims, eligibility, and payment data through receipt of an accreditation by the Electronic Healthcare Network Accreditation Commission, or

by an equivalent accreditation program determined appropriate by the Secretary.

"(3) ENHANCING TREATMENT, QUALITY IMPROVEMENT, RESEARCH, PUBLIC HEALTH EFFORTS AND OTHER FUNCTIONS.—

"(A) EQUIVALENT AUTHORITY TO OTHER COVERED ENTITIES.—Subject to paragraph (2), a health care clearinghouse shall—

"(i) in addition to carrying out claims processing functions, be permitted to use and disclose protected health information without obtaining individual authorization to the same extent as other covered entities, including for purposes of treatment, payment, health care operations as permitted by section 164.506 of title 45, Code of Federal Regulations, research, and public health as permitted by section 164.512 of title 45, Code of Federal Regulations, and creating de-identified information as permitted by section 164.502(d) of title 45, Code of Federal Regulations; and

"(ii) use or disclose protected health information as required by section

164.502(a)(2) of title 45, Code of Federal Regulations.

"(B) ADDITIONAL AUTHORITY.—

"(i) A health care clearinghouse shall be permitted to provide an individual or the personal representative of such individual access to the protected health information of such individual as described in subsection (d).

"(ii) All covered entities, including a health care clearinghouse, shall, subject to subsection (c)(2), be permitted to—

"(I) on behalf of covered entities, use and disclose protected health information for health care operations purposes (as defined by section 164.501 of title 45, Code of Federal Regulations) without respect to whether the recipient of the information has or had a relationship with the individual;

"(II) upon the request of a covered entity, benchmark (as defined by the Secretary pursuant to rulemaking) the operations of such covered entity

against the operations of one or more other covered entities that have elected to participate in such benchmarking; and

"(III) use and disclose protected health information to facilitate clinical trial recruitment, except that in the case the covered entity provides a consumer-facing portal or website that informs individuals of clinical trials conducted by the covered entity, the covered entity shall secure opt-in consent from the individual, or the individual's personal representative, prior to contacting an individual regarding such clinical trials unless such covered entity already has a relationship with the individual.

"(C) CLARIFICATION.—Nothing in this paragraph shall expand the authority of a health care clearinghouse or any other covered entity to use or disclose protected health information for marketing purposes under sections 164.501 and 164.508(a)(3) of title 45, Code of Federal Regulations.

"(c) AUTHORITIES RELATING TO DATA PROCESSING.—

"(1) IN GENERAL.—In carrying out HIPAA-related provisions, the Secretary shall permit a health care clearinghouse to aggregate protected health information, within the clearinghouse and among other clearinghouses, that the clearinghouse possesses in order to carry out the functions described in subsection (b)(3). Subject to section 164.502(a)(5)(i) of title 45, Code of Federal Regulations, a health care clearinghouse may carry out the functions described in subsection (b)(3) without obtaining individual authorization under section 164.508 of title 45, Code of Federal Regulations.

"(2) PRIVACY.—For purposes of clauses (ii) through (iv) of subsection (b)(3)(B), with respect to any report, analysis, or presentation provided by the covered entity to a third party, such report, analysis, or presentation—

"(A) shall include only de-identified data; or

"(B) shall include, subject to a qualifying data use agreement (as defined in subsection (j)), protected health information.

"(3) CLARIFICATION; FEE PERMITTED.—

"(A) IN GENERAL.—Nothing in this paragraph shall be construed as affecting an individual's right to access claims and payment records in HIPAA standard format, in accordance with section 164.524 of title 45, Code of Federal Regulations.

"(B) FEE PERMITTED.—If an individual or a personal representative of the individual requests a copy of records in HIPAA standard format a health care clearinghouse may charge a reasonable, cost-based fee so far as such fee is in accordance with section 164.524(c)(4) of title 45, Code of Federal Regulations.

"(d) COMPREHENSIVE RECORDS AT THE REQUEST OF AN INDIVIDUAL.—

"(1) IN GENERAL.—When a health care clearinghouse receives a written request from an individual or the personal representative of the individual for the protected health information of the individual, the clearinghouse shall provide to the individual a comprehensive record of such information (across health care providers and health plans and longitudinal in scope), unless the clearinghouse determines in its sole discretion that providing a comprehensive record is not technologically feasible.

"(2) PURCHASE FROM OTHER CLEARINGHOUSES.—In preparing a comprehensive record for an individual under paragraph (1), a health care clearinghouse may, with the permission of the individual, purchase the protected health information of the individual from one or more other health clearinghouses (and the amount of such purchase may be included in a fee that is fair market value, as defined in subsection (j)(2), charged to the individual.

"(e) SITUATIONS NOT INVOLVING DIRECT INTERACTION WITH INDIVIDUALS.—Sections 164.400 through 164.414 (relating to breach notification) and sections 164.520 through 164.528 (relating to individual rights) of title 45, Code of Federal Regulations, shall apply to a health care clearinghouse that engages in the functions described in subsection (b)(3) to the extent that such clearinghouse has current contact information pursuant to direct interaction with the individual involved. If the clearinghouse does not have direct interaction with the individual involved, the clearinghouse shall provide notice of any breach of unsecured protected health information to the covered entity that does have direct interaction with the individual involved. The clearinghouse shall not be required to report a breach if the protected health information is rendered unusable, unreadable, or indecipherable

to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2). The clearinghouse shall also provide a notice of privacy practices on its website.

"(f) TRANSITION.—

"(1) IN GENERAL.—Except where specifically stated, nothing in this section shall be construed to apply to clearinghouses to the exclusion of other covered entities or to provide a health care clearinghouse greater authority to use and disclose protected health information than that provided to another covered entity.

"(2) EXISTING AGREEMENTS.—With respect to agreements entered into by a health care clearinghouse prior to the date of enactment of this section, a provision of such an agreement that conflicts with this section shall not have any legal force or effect. The preceding sentence may not be construed as affecting any provision of an agreement that does not conflict with this section.

"(g) SAFE HARBOR AND CLARIFICATION OF LIABILITY.—In the case of a health care clearinghouse that engages in a function described in subsection (b), only that clearinghouse may be held liable for a violation of a HIPAA-related provision (and a covered entity that pro-

vided data or data access to the clearinghouse shall not be liable for such violations).

"(h) ENFORCEMENT.—Section 13410(a)(2) shall apply to this section in the same manner as such section applies to parts 1 and 2.

"(i) RELATION TO OTHER LAWS.—

"(1) APPLICATION OF HITECH RULE.—Section 13421 shall apply to this section in the same manner as such section applies to parts 1 and 2, except to the extent that such section 13421 concerns section 1178(a)(2)(B) of the Social Security Act.

"(2) STATE LAWS REGARDING UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—This part shall not be construed to preempt the law of any State that prohibits unfair or deceptive acts or practices or limit the authority of State attorneys general to enforce such laws.

"(j) DEFINITIONS.—In this part:

"(1) DE-IDENTIFIED.—The term 'de-identified', with respect to health information, means such information that is not individually identifiable as determined in accordance with the standards under section 164.514(b) of title 45, Code of Federal Regulations.

"(2) FAIR MARKET VALUE.—The term 'fair market value' means the price that a person reasonably knowledgeable and interested in buying a given product or service would pay to a person reasonably knowledgeable and interested in selling the product or service.

"(3) HEALTH CARE CLEARINGHOUSE.—The term 'health care clearinghouse' has the meaning given such term in section 1171 of the Social Security Act.

"(4) HIPAA-RELATED PROVISION.—The term 'HIPAA-related provision' means the provisions of each of the following:

"(A) This subtitle.

"(B) Part C of title XI of the Social Security Act.

"(C) Regulations promulgated pursuant to sections 262(a) and 264(c) of the Health Insurance Portability and Accountability Act of 1996 or this subtitle.

"(5) INDIVIDUAL.—The term 'individual', with respect to protected health information, has the meaning applicable under section 160.103 of title 45, Code of Federal Regulations.

"(6) QUALIFYING DATA USE AGREEMENT.—The term 'qualifying data use agreement' means an agreement, which may be electronic, that—

"(A) establishes the permitted uses and disclosures of protected health information by the recipient;

"(B) limits such uses and disclosures to the original purpose of disclosure under subsection (b)(3)(B); and

"(C) provides that the data recipient will—

"(i) not use or further disclose the information other than as permitted by the qualifying data use agreement or as otherwise required by law;

"(ii) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the qualifying data use agreement; and

"(iii) ensure that any agents to whom it provides the data agree to the same restrictions and conditions that apply to the data recipient with respect to such information.".

(b) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of

Health and Human Services shall promulgate regulations to carry out the amendment made by subsection (a).

(c) CONFORMING AMENDMENT.—Section 1171(2) of the Social Security Act (42 U.S.C. 1320d(2)) is amended by inserting before the period the following: "or receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. Such term also includes an entity that carries out such processing functions, transmits standard health care claims, transmits health care claim payments or provides advice on such, and transmits any standard transactions on behalf of a HIPAA-covered entity and in addition, engages in any authority of such entity described in subsection (b)(3) of section 13451 of the Health Information Technology for Economic and Clinical Health Act".

○

Attachment 2

Privileged & Confidential
Attorney Work Product

Ensuring Patient Access to Healthcare Records Act

1. Health care clearinghouses would ***gain greater latitude*** to buy, use, and disclose Protected Health Information ***than health plans and health care providers*** and than other business associates.
    - *Clearinghouses* are large data brokers that process or facilitate the processing of patients' health information, such as claims.
    - *Protected Health Information* (PHI) is individually identifiable health information transmitted or maintained electronically, orally, or on paper.
    - Clearinghouses would need to become accredited and perform certain functions.

2. Some of HIPAA's ***privacy protections for PHI and individuals would be eliminated***.
    - If an accredited clearinghouse engages in certain functions, the bill would invalidate protections for PHI in existing agreements with plans, providers, and other entities.
    - If a clearinghouse does not have current contact information for an individual because of a "direct interaction" with that individual, the clearinghouse would not have to follow HIPAA regulations that grant individuals rights, such as the right to know with whom their PHI has been shared with which health plans and health care providers must comply.

3. Many ***at-risk individuals would not be notified*** if the clearinghouse that held their information experienced a ***HIPAA breach***, such as a ransomware attack.
    - An accredited clearinghouse engaging in certain functions would only need to notify individuals for whom the clearinghouse has current contact information pursuant to a direct interaction with the individual.
    - Given a clearinghouse's role as a data broker, it is unlikely that a clearinghouse would have many "direct interactions" with individuals.
    - It is unclear if the at-risk individuals would receive any notice of the breach and if the clearinghouse would need to report the breach to HHS and the media.

4. The bill would ***preempt state laws*** that provide stronger privacy protections for individually identifiable health information.
    - The bill does not limit the more stringent state laws that would be preempted, for example, laws protecting HIV+ status or genetic information.
    - The bill may preempt state laws that prohibit unfair or deceptive practices if such laws relate to the privacy of health information.

5. Only ***clearinghouses would be able to buy health information*** from other clearinghouses and prepare comprehensive records requests.
    - Health plans and health care providers could not buy such information.
    - The bill is inconsistent as to whether plans and providers could prepare such reports.

6. An individual's permission would not be required for a clearinghouse to aggregate PHI across multiple clearinghouses in order to perform functions such as clinical trial recruitment.

7. The bill purports to restrict a clearinghouse's use and disclosure of genetic information, but the cross-referenced protections for genetic information do not apply to clearinghouses.

Clearinghouse Trying to Break into Health Information Exchange Business

Alex Ruoff

Availity, one of the country's largest health insurance clearinghouses, is backing proposed changes to federal privacy laws in hopes of expanding its information exchange services.

The company's top executive told me he wants clearinghouses like his to be treated similarly to hospitals or doctors under Health Insurance Portability and Accountability Act (HIPAA) rules for sharing health data, which could solve some of the health industry's data-exchange problems. He and other supporters are backing bills in the House and Senate would make such changes.

Clearinghouses hold some of the largest stores of clinical data and want to make that data available to doctors around the country to help them better serve their patients, Russ Thomas, chief executive officer of Availity, told me. However, he said, clearinghouses—which connect health-care providers to insurers to process claims—are hamstrung by HIPAA, which prohibits them from sharing health data like hospitals and doctor's offices can.

"Right now we move billions of bits and bytes, but only to certain people and organizations," Thomas said. "We could find new ways to use this information in valuable ways."

Thomas and Anna Spencer, a lobbyist with Sidley Austin LLP, came to Washington recently to support several pending bills, including the House's 21st Century Cures Act (H.R. 6) and the Senate companion bill, as well as the Ensuring Patient Access to Healthcare Records Act of 2016 (H.R. 4805).

Both Thomas and Spencer cited the Ensuring Patient Access to Healthcare Records Act—introduced March 7 by Rep. Cathy McMorris Rodgers (R–Wash.)—as essential to making it easier for health-care organizations to access patient records. The bill would alter HIPAA to specify that clearinghouses should be treated as covered entities under the law, according to an outline of the billpublished by McMorris Rodgers.

Congress holds the key to achieving improved healthcare through better use of data

How a simple change in federal law could finally make way for comprehensive medical records

By: Dan Johnson
Sep 26, 2017

Valuable data is on HIPAA lockdown

Congress passed the Healthcare Information Portability and Accountability Act (HIPAA) in 1996 to ensure data privacy and security for medical information. The Privacy Rule implementing HIPAA applies to "covered entities" like health plans, healthcare clearinghouses, and certain healthcare providers. Under HIPAA, providers and plans may disclose protected health information to "business associates" that provide specific services. This means that when healthcare clearinghouses are engaging in activities like claims processing, they're defined under the rule as both a covered entity and a business associate.

Clearinghouses handle an estimated 90% of all healthcare claims transactions in the United States. These companies have existed for decades—long before the idea that consumers should have access to their EHRs. Clearinghouses manage payment transactions that flow between payers and more than 5,000 hospitals, 900,000 doctors, 66,000 pharmacies, and 20,000 labs.

HIPAA's dual restrictions on healthcare clearinghouses limit the use of this data for any purpose except processing claims. The result is that clearinghouses are prevented from playing a role in helping patients and providers easily obtain a full and historical view of healthcare visits, diagnosis, and treatment. The Ensuring Patient Access to Healthcare Records Act would allow clearinghouses to lead this effort.

Notably, the regulators who drafted the original HIPAA Privacy Rule in 1999 anticipated the restrictive nature of the business associate status for clearinghouses. The preamble of the proposed HIPAA rule noted, "As technology improves it is likely that clearinghouses will find ways to take advantage of databases of protected health information that aggregate records based on the individual subject of the information. This technology would allow more cost-effective access to clearinghouse records on individuals and therefore access for inspection and copying could be appropriate and reasonable."

Legislation would remove the BA designation from clearinghouses

The technology for achieving data portability of comprehensive healthcare records envisioned by regulators nearly 20 years ago is achievable today if Congress enacts the Ensuring Patient Access to Healthcare Records Act. The act would help realize the benefit of interoperable health data that the government sought to achieve with the HITECH Act, EHRs, and other post-HIPAA programs.

The legislation would clarify that healthcare clearinghouses, regardless of their original status as a business associate under HIPAA, should be permitted to use and disclose protected health information in the same manner as other covered entities under the HIPAA Privacy Rule. This would let clearinghouses distribute data for all permitted uses under HIPAA while still ensuring that they meet the privacy and data security requirements of current law.

Patient matching technology would be improved

An effective patient matching technology could mean immense savings and efficiencies for our nation's healthcare system. In 2008, the RAND Corporation estimated that such technology would deliver $77 billion in savings through error reduction, efficiency, and interconnectivity.

To create an environment of data portability, archived data from multiple clearinghouses would be linked through a non-vendor-specific universal patient identifier (UPI)

algorithm. A UPI would associate all relevant health data with a unique individual, providing for the compilation of accurate medical histories that can flow throughout the healthcare ecosystem. This data would lead to not only tangible benefits to patients, but also to better public health outcomes, such as cost savings for payers and providers and a reduction in healthcare fraud and medical identity theft.

Improved data matching through a UPI would also help resolve a common problem that plagues our nation's health system—a patient receiving the wrong diagnosis or lab results after being mistaken for another patient with the same name. Such problems lead to unnecessary treatments and surgeries that only further drive up costs for patients, providers and insurers.

Patients would benefit from a comprehensive view of their medical history

Patients would also benefit if the business associate designation for clearinghouses is removed. Their demand for access to their own health information could finally be met with the compiled historical data that clearinghouses could make available to patients, payers, and providers.

Just imagine patients being able to easily access their personal medical history, including dates of service, diagnoses and treatments for every healthcare event going back decades. This would replace the fractured and siloed nature of our current healthcare information environment with a seamless, interoperable system. Patients would no longer face the daunting task of assembling their healthcare history by relying on memory or spending an inordinate amount of time piecing together their medical history by requesting records from individual providers through fax or mail.

Providers would see reduced costs, improved efficiencies and better healthcare outcomes

With the business associate designation removed, clearinghouses would initially be able to provide a medical history checking system that healthcare providers could access through revenue cycle management products or an online portal. Data could also be

provided in a virtual clearinghouse and integrated into health information systems and practice management systems. That way, providers could query a patient's historical data consistent with their own preferred workflow process.

This would solve the challenge healthcare providers face with duplicate records. A hospital or doctor would now know me, Dan Johnson, from all the other Dan Johnsons who have received services from a doctor or hospital somewhere at some time over the past decades. My complete medical history, across all providers I've visited, could be used in clinical decisions. Think about all the time and resources healthcare providers spend trying to distinguish one Dan Johnson from another. Then, imagine the productivity that can be gained when these resources can instead be put to use improving clinical decisions.

Clearinghouses are already helping individual health systems create unique identifiers for their patients. However, productivity could be further enhanced if healthcare providers and clearinghouses could share data using the same UPI across enterprises.

The pharmacy industry is already pursing this effort. In 2016, the National Council for Prescription Drug Programs (NCPDP) partnered with Experian Health to standardize patient identifiers for the billions of transactions flowing through the pharmacy systems to solve the same duplicate records problem that confronts healthcare providers.

Coalition supports reform

A coalition of leading healthcare clearinghouses is actively supporting enactment of the Ensuring Patient Access to Healthcare Records Act and working to educate lawmakers and policymakers about the many ways the act would benefit patients and healthcare providers.

The Claim Your Health Data Coalition was established in 2016 by The SSI Group, Availity, and Experian Health and is committed to advancing the cause of unlocking the potential for data currently siloed within clearinghouse networks. Together, these three

companies process hundreds of millions of individual claims safely and securely every year.

When she introduced the legislation in March 2016, Rep. McMorris Rodgers said, "By allowing patients to have access to their own comprehensive medical records, we can lower healthcare costs, address market inefficiencies and otherwise improve our health systems."

It's been said that "data is the new oil." It's time for Congress to ensure that data can be used responsibly and securely to drive real and positive improvement in healthcare delivery.

Attachment 5

New Bill to Improve Patient Access to Health Information

Bill would enable patient access to health information that is comprehensive and longitudinal.

By Kate Monica

December 22, 2017 - Congresswoman Cathy McMorris Rodgers (WA-05) **recently introduced** a bipartisan bill intended to give medical record clearinghouses the ability to improve patient access to health information as well as makes claims data available for analysis that benefits public health.

The Ensuring Patient Access to Healthcare Records Act allows clearinghouses to link health data and build longitudinal records to ensure patients have a comprehensive medical record.

"Even in the age of technology, it can be difficult for patients to obtain their comprehensive health records," said McMorris Rodgers. "Whether it's because of a move to a new state, switching providers, an unexpected visit to the emergency room, or a new doctor, patients must track down their own records from numerous different sources based on what they can or cannot remember."

Medical record clearinghouses process hundreds of millions of transactions from more than 5,000 hospitals, 900,000 providers, 66,000 pharmacies, and 20,000 labs across the country each year. Records contained in medical clearinghouses include information about diagnoses, medical treatment, and healthcare providers for each patient-provider interaction.

"Claims data could be analyzed by clearinghouses both longitudinally and geographically, providing powerful analytical tools that could benefit the overall healthcare system and facilitate medical innovation in the 21st Century," stated McMorris Rodgers in a **one page summary** of the legislation.

The legislation will also assist pharmaceutical companies by allowing them access to information useful for outlining the company's market potential. Specifically, pharmaceutical companies can outline the population of patients that may be helped by a new treatment. Additionally, information in clearinghouses can identify potential patients that may be eligible for enrollment in clinical trials.

Clearinghouses have the capabilities to analyze healthcare data to address public policy goals by tracking patient health outcomes across the care continuum. Additionally, clearinghouses can assist with tracking significant disease outbreaks and epidemics.

"It shouldn't be this burdensome," McMorris stated. "Our bill gives patients the ability to see a snapshot of their health records at just a simple request, allowing them to make better, more informed healthcare decisions in a timely manner."

Presently, HIPAA restricts clearinghouses from providing patients with longitudinal health records or allowing stakeholders access to information obtained by analyzing patient health outcomes. This new legislation introduced by McMorris Rodgers is an effort to allow patients in Eastern Washington full access to their health data despite the limitations imposed by HIPAA.

The act "would clarify that regardless of whether a clearinghouse originally collected Protected Health Information (PHI) in its role as a business associate, the clearinghouse is permitted to use and disclose PHI in the same manner as other covered entities under the Privacy Rule," according to McMorris Rodgers.

"These uses and disclosures include: research purposes, public health purposes, and releasing the individual's own PHI to said individual," McMorris Rodgers continued.

Public health authorities including FDA, CDC, state health departments, and other public health entities also stand to benefit if the legislation is passed. These entities will gain the ability to collect and receive health information from medical clearinghouses to prevent or control disease, injury, or disability among patient populations.

"Additionally, the legislation would permit a clearinghouse to analyze, prepare, and distribute reports with the goals of improving healthcare; lowering healthcare costs; identifying and addressing market inefficiencies; facilitating public health monitoring, and otherwise improving the healthcare system," she wrote.

Introducing the Ensuring Patient Access to Healthcare Records Act is an attempt to further the aims of the 21st Century Cures Act by improving patient access to health data.

Attachment 6

Mar 17, 2016

MCMORRIS RODGERS INTRODUCES ENSURING PATIENT ACCESS TO HEALTHCARE RECORDS ACT

Eastern Washington Congresswoman Cathy McMorris Rodgers, Chairwoman of the House Republican Conference, released the following statement after introducing the Ensuring Patient Access to Healthcare Records Act.

"As we create a 21st Century health care system that puts patients in charge of their health care decisions, this is an important step forward in ensuring transparency and access," said McMorris Rodgers. "By allowing patients to have access to their own comprehensive medical records, we can lower healthcare costs, address market inefficiencies, and otherwise improve our health systems."

The Ensuring Patient Access to Healthcare Records Act would clarify that a clearinghouse is permitted to use and disclose Protected Health Information (PHI) in the same manner as other covered entities under the Health Insurance Portability and Accountability Act (HIPPA) including for research purposes, public health purposes, and releasing an individual's own PHI to said individual. To ensure the continued security of these activities, the bill would maintain all criminal and civil liabilities currently prescribed by HIPAA to safeguard the privacy of individuals

Attachment 7

The Office of the National Coordinator for Health Information Technology

JANUARY 5, 2018

DRAFT FOR PUBLIC COMMENT

DRAFT TRUSTED EXCHANGE FRAMEWORK

CONTENTS

Introduction

Overview[1]

While the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 stimulated significant health information technology (health IT) adoption and exchange of Electronic Health Information with the goal of every American having access to their Electronic Health Information, the interoperability experience remains a work in progress. The 21st Century Cures Act's (Cures Act) [2] focus on trusted exchange is an important next step toward advancing the establishment of an interoperable health system that:

- Empowers individuals to use their Electronic Health Information to the fullest extent;
- Enables providers and communities to deliver smarter, safer, and more efficient care; and
- Promotes innovation at all levels.

The vision we seek to achieve is a system where individuals are at the center of their care and where providers have the ability to securely access and use health information from different sources. A system where an individual's health information is not limited to what is stored in electronic health records (EHRs), but includes information from many different sources (including technologies that individuals use every day) and provides a longitudinal picture of their health. Additionally, we seek a system where public health agencies and researchers can rapidly learn, develop, and deliver cutting edge treatments by having secure, appropriate access to Electronic Health Information. [3]

Currently, there are more than 100 regional health information exchanges (HIEs)[4] and multiple national level organizations that support exchange use cases. While these organizations have expanded

---

[1] Please note that all capitalized terms throughout the document have the meaning set forth in Part B Definitions.

[2] Pub. L. 114–255 (Dec 13, 2016).

[3] Electronic Health Information" (EHI) means any information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. EHI includes information that is accessed, exchanged, used or maintained in the context of the Trusted Exchange Framework and may be developed for an individual, on behalf of an individual, or provided directly from either an individual or from technology that the individual has elected to use. EHI includes but is not limited to ePHI and health information as defined in 45 CFR 160.103. However, unlike ePHI and health information, EHI is not limited to information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university or health care clearinghouse. EHI does not include health information that is de-identified consistent with the requirements of 45 CFR 164.514(b).

[4] Julia Adler-Milstein, Sunny C. Lin, and Ashish K. Jha. The Number Of Health Information Exchange Efforts Is Declining, Leaving The Viability Of Broad Clinical Data Exchange Uncertain. Health Affairs Vol. 35 No. 7: July 2016. https://doi.org/10.1377/hlthaff.2015.1439

interoperability within their particular spheres, the connectivity across all or even most of them has not been achieved. This has limited the patient health information that a provider or health system has access to, unless they join multiple networks. In fact, a recent survey of about 70 hospitals found that few hospitals used only one method to be interoperable. A majority of surveyed hospitals required three or more methods and about three in 10 hospitals used five or more methods.[5] While some of these networks have begun to connect with each other, interoperability between these organizations has been limited and subject to variations in the participation agreements that govern exchange.

In the Cures Act, Congress identified the importance of interoperability and laid out a path for the establishment of interoperable exchange of Electronic Health Information. In collaboration with the National Institute of Standards and Technology (NIST), federal agencies, and industry stakeholders, the Office of the National Coordinator for Health IT (ONC) is working diligently to further advance the interoperability progress made to date and address the complex yet core tenet of interoperability—building and maintaining trust. Among other provisions, in Section 4003, Congress directed ONC to "develop or support a trusted exchange framework, including a common agreement among health information networks nationally," which may include:

"(I) a common method for authenticating trusted health information network participants;

"(II) a common set of rules for trusted exchange;

"(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and

"(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement.[6]

As part of ONC's implementation of Section 4003, we have held three listening sessions with a wide range of stakeholders, completed one round of public comment, and met with a variety of stakeholders. We appreciate Congress' recognition of the need for a trusted exchange framework and common agreement, and the provisions in the Cures Act provide the means to build on the industry's commitment to increasing trust across networks, while ensuring the privacy, security, and appropriate use of Electronic Health Information[7] when and where it is needed. We look forward to the public's engagement as we move forward with implementing the Trusted Exchange Framework and Common Agreement (TEFCA)[8] provisions and to your feedback on the draft Trusted Exchange Framework.

---

[5] Jordan Everson, PhD. "Measuring the Interoperability Network" Presented at ONC Annual Meeting, November 30, 2017. Washington, D.C.

[6] Id.

[7] The terms "health information," "health data," and "data" are synonymous in the context of the TEFCA and refer to all electronic health-related data for a patient. Specific references to ePHI refer to the HIPAA definitions of electronic protected health information and protected health information (PHI).

[8] All capitalized terms or acronyms used in Part A without definition shall have the respective meanings assigned to such terms in Part B, Section 1 below.

Trusted Exchange Framework's Relationship to HIPAA

As part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA Privacy Rule covers health plans, health care clearinghouses, and healthcare providers who conduct certain financial and administrative transactions electronically.[9] These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers. These entities (collectively called "Covered Entities") are bound by the privacy and security standards even if they contract with others (called "Business Associates") to perform some of their essential functions.

A Business Associate is a person or entity, other than a member of the workforce of a Covered Entity, who performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to protected health information.[10] A Business Associate also is a subcontractor that creates, receives, maintains, or transmits protected health information (PHI) on behalf of another Business Associate. The HIPAA Rules generally require that Covered Entities enter into contracts with their Business Associates to ensure that the Business Associates will appropriately safeguard PHI. The Business Associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the Business Associate, based on the relationship between the parties and the activities or services being performed by the Business Associate. A Business Associate may use or disclose PHI only as permitted or required by its Business Associate contract or as required by law.

A Covered Entity's contract or other written arrangement with its Business Associate must contain the minimum elements specified at 45 C.F.R. 164.504(e). For example, the contract must: describe the permitted and required uses of PHI by the Business Associate; provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and require the Business Associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.

Health Information Networks (HINs) typically operate as Business Associates and currently have Business Associate agreements, otherwise known as participation agreements, in place with their Participants. These agreements facilitate the exchange of Electronic Health Information since they perform functions or activities on behalf of, or provide certain services for Covered Entities such as determining and administering policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of health information between or among two or more Covered Entities. Additionally, a Qualified Health Information Network (Qualified HIN), a HIN that has agreed to the terms set forth in the Common Agreement, also operates as a Business Associate to its Participants, but Qualified HINs may also have Participants who are not themselves Covered Entities or Business Associates.

---

[9] 45 C.F.R. 160.103

[10] Id.

We have worked with the HHS Office of Civil Rights (OCR) to ensure that the proposed Trusted Exchange Framework aligns with HIPAA and does not contradict HIPAA requirements. However, we anticipate that many end users may not be Covered Entities or Business Associates as defined by HIPAA, and the final TEFCA must be broad enough to enable them to appropriately and securely access health information. Therefore, while the proposed Trusted Exchange Framework aligns with HIPAA requirements, it also specifies terms and conditions to enable broader exchange of health information. This is not a new reality for most HINs, and we understand that most have participation agreements that utilize broader terms to enable both covered and non-Covered Entities to utilize their networks.

An "On-Ramp" to Data Liquidity

The Draft Trusted Exchange Framework recognizes the significant work done by the industry over the last few years to broaden the exchange of data to meet the needs of patients and the providers who serve them, build trust frameworks, and develop participation agreements that enable stakeholders to exchange data across organizational boundaries. The draft Trusted Exchange Framework also recognizes that not all networks serve the same stakeholders or use cases[11] and have, in many cases, tailored their frameworks to meet the needs of their participants and their prioritized use cases.

Through our exploration of existing networks, we have heard stakeholders' concern regarding the creation of a single HIN that is intended to address all the needs of all stakeholders and comprehensively address all use cases.[12] At this time, a single network is not feasible, since there are technical limitations, security concerns, variations in the participants being served in use cases, and resource limitations for each network. However, establishing a single "on ramp" to Electronic Health Information that works regardless of one's chosen network is feasible and achievable.

To scale interoperability nationwide and ensure that patients, providers across the care continuum, community and social services, and many more stakeholders can effectively and efficiently participate in interoperability, our goal is to use the successes in the industry to create the single "on-ramp" we seek. To that end, the Trusted Exchange Framework focuses on policies, procedures, and technical standards that build from existing HIN capabilities and enables them to work together to provide that single "on-ramp" to Electronic Health Information regardless of what health IT developer they use, health information exchange or network they contract with, or how far across the country the patients' records are located. At the same time, this "on-ramp" will still allow HINs to innovate and build out additional use cases and services that would provide value to their Participants and support their long-term sustainability.

---

[11] Use case refers to particular services a network may provide or workflows it may support. Examples of use cases include but are not limited to notification services, quality measurement services, analytics services, connectivity services, appropriate patient access, etc.

[12] See https://www.healthit.gov/sites/default/files/tefca_public_comments_as_of_2017_08_28_final_xlsx.xlsx

While we applaud the progress made to date and the hard work each organization has contributed to move the industry forward, additional and faster progress must be made; this is particularly true in the case of medical specialties—such as long-term services and supports (LTSS)[13] providing post-acute care or in lieu of institutionalization, behavioral health, and other ambulatory services. Continuing with the status quo will not be enough to ensure these stakeholders have efficient methods for engaging in health information exchange. The Trusted Exchange Framework's minimum set of policies, procedures, and technical standards are intended to advance interoperability, particularly with these stakeholders, and enable them to use HINs to support the many use cases that are important to them and their patients (clients), including the exchange of data for Treatment, Payment, Health Care Operations (TPO)[14], Individual Access, Public Health,[15] and Benefits Determination.[16] We believe that the proposed Trusted Exchange Framework supports the interoperability goal of reliable information flowing to enable communication among services that make use of Electronic Health Information, ultimately providing stakeholders with greater choice.

In an effort to develop and support a trusted exchange framework for trusted policies and practices and for a common agreement for the exchange between HINs, the proposed Trusted Exchange Framework supports four important outcomes: 1) providers can access health information about their patients, regardless of where the patient received care; 2) patients can access their health information electronically without any special effort; 3) providers and payer organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on a group of individuals without having to access one record at a time (Population Level Data),[17] which would allow them to analyze population health trends, outcomes, and costs; identify at-risk populations; and track progress on quality improvement initiatives; and 4) the health IT community has open and accessible application programming interfaces (APIs) to encourage entrepreneurial, user-focused innovation to make health information more accessible and to improve electronic health record (EHR) usability.[18] All four of these outcomes shall be accomplished in compliance with applicable HIPAA Rules' requirements.

---

[13] See https://www.medicaid.gov/medicaid/ltss/index.html for a definition of LTSS.

[14] A Covered Entity or Business Associate may use or disclose electronic protected health information without an individual's authorization for its own treatment, payment or health care operations as defined under the HIPAA Privacy Rule. See 45 C.F.R. §164.501 and 45 C.F.R. §164.506.

[15] Public health is defined as with respect to the definition of Permitted Purposes, a use or disclosure permitted under the HIPAA Regulations and any other Applicable Law for public health activities and purposes, including, without limitation, 45 C.F.R. §164.512(b) and 45 C.F.R. §164.514(e) of the HIPAA Regulations.

[16] Benefits determination is defined as a determination made by any federal or state agency that an individual qualifies for federal or state benefits for any purpose other than health care (for example, Social Security disability benefits).

[17] Population Level: a type of exchange of Electronic Health Information of multiple individuals in a single transaction, sometimes referred to as a bulk transfer.

[18] Under Section 4002 of the Cures Act, the Secretary is required under rulemaking to publish application programming interfaces that allows health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, as provided for under Applicable Law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

In addition, the Trusted Exchange Framework focuses on broadly applicable use cases that are discussed further below. The use cases identified are structured to address the areas of greatest need while also allowing existing HINs and trust frameworks to vary as appropriate to meet more specialized use cases that are specific to their own Participants. We believe that this approach will significantly reduce the need for multiple point-to-point interfaces. As stakeholders noted during the public comment process, these interfaces are costly, complex to create and maintain, and an inefficient use of provider and health IT developer resources. It should be noted that while the Trusted Exchange Framework is structured to create a single "on-ramp" for the most common exchange use cases, it does not prevent organizations from creating point-to-point or one-off agreements between organizations who have a particular business need to exchange data in a manner that is different from the minimum set of policies, procedures, and technical standards outlined in the Trusted Exchange Framework, provided that such agreements do not undermine the policies of the Trusted Exchange Framework.[19]

To achieve the "on-ramp" ONC has identified, there are steps that must be taken to ensure that networks that are responsible for the flow of Electronic Health Information follow a minimum set of policies, procedures, and technical standards to enable the use of that data for the broadest set of use cases possible—the use cases that all stakeholders will benefit from. The provisions in the Trusted Exchange Framework are necessary for patient care, care coordination, and the overall health of the population and can only be successful with the participation of—for example—existing networks, health IT developers, and federal agencies.

While we recognize that the provisions we have laid out in the Trusted Exchange Framework will necessitate modifications to existing participation agreements and trust frameworks to support provisions such as the additional permitted disclosures of health information by the Qualified HINs, we believe that these changes are necessary for us to meet the objectives identified by Congress and will enable providers and patients to have a single "on-ramp" to exchange.

We believe that we can move quickly towards nationwide interoperability, but we recognize that we cannot achieve interoperability alone. We look forward to the health IT stakeholder community joining us on this journey.

---

[19] The HIPAA Privacy Rule generally requires Covered Entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose unless an exception applies such as for treatment purposes. In certain circumstances, the HIPAA Privacy Rule permits a Covered Entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by: a public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 C.F.R. §164.512 of the Rule, such as for public health purposes (45 C.F.R. §164.512(b)), another Covered Entity or a professional who is a workforce member or Business Associate of the Covered Entity holding the information and who states that the information requested is the minimum necessary for the stated purpose. See generally, 45 C.F.R. §164.502 and 45 C.F.R. §164. 514.

How Will It Work?

This Draft Trusted Exchange Framework contains two parts: Part A – Principles for Trusted Exchange and Part B – Minimum Required Terms and Conditions for Trusted Exchange. Part A provides guard rails and general principles that Qualified HINs and HINs should follow to engender trust amongst Participants and End Users. Part B provides specific terms and conditions that will be incorporated into a single Common Agreement by a Recognized Coordinating Entity (RCE). Subsequently, ONC will publish on our public website and in the Federal Register the TEFCA, which is the combination of the Trusted Exchange Framework and the Common Agreement.

ONC intends to select through a competitive process a single RCE that will incorporate the Part B requirements into a single Common Agreement to which Qualified HINs may voluntarily agree to abide. The RCE will be tasked with operationalizing the Trusted Exchange Framework. We believe that a single, industry-based RCE is best positioned to operationalize the Trusted Exchange Framework. Implementing the TEFCA requires day-to-day management and oversight of unaffiliated Qualified HINs, including: onboarding organizations to the final TEFCA, ensuring Qualified HINs comply with the terms and conditions of the TEFCA, addressing non-conformities with Qualified HINs, developing additional use cases, updating the TEFCA over time, and working collaboratively with stakeholders. ONC intends to work closely with the RCE and to be continually involved in implementation of the TEFCA. We look forward to stakeholder comment on this approach.

Because the RCE will be tasked with operationalizing the Trusted Exchange Framework, we have chosen in Part B to focus solely on provisions that are currently variable across HINs and that prevent the exchange of Electronic Health Information between HINs. Part B is not intended to be an all-encompassing participation agreement. To operationalize the Trusted Exchange Framework, the RCE will incorporate additional, necessary provisions into the Common Agreement as long as such provisions do not conflict with the Trusted Exchange Framework, as approved by ONC. The RCE will be expected to monitor Qualified HINs compliance with the Common Agreement and take actions to address any non-conformity with the Common Agreement—including the removal of a Qualified HIN from the Common Agreement and subsequent reporting of its removal to ONC. The RCE will also be expected to work collaboratively with stakeholders from across the industry to build and implement new use cases that can use the TEFCA as their foundation, and appropriately update the TEFCA over time to account for new technologies, policies, and use cases.

ONC believes that a private-sector organization would be best positioned to serve as the RCE and, to that end, we intend to release an open and competitive Funding Opportunity Announcement (FOA) in spring 2018 to award a single, multi-year Cooperative Agreement to an RCE. The multi-year Cooperative Agreement will allow ONC to closely collaborate with the RCE to help ensure that the final TEFCA supports all stakeholders and that interoperability continues to advance. In general, we believe the RCE will need to have experience with building multi-stakeholder collaborations and implementing governance principles. The FOA announcement will provide additional specificity on the eligibility criteria that an applicant would have to meet to be chosen as the RCE.

The voluntary adoption by Qualified HINs of the Common Agreement may require that each network make upgrades to its health IT capabilities and align to certain trust and operational practices. Over time, and with the approval of ONC, the RCE will update the Common Agreement as necessary to account for new technical standards and policy requirements. ONC will work with the RCE to develop and/or implement a process for such updates.

Qualified HINs that voluntarily adopt the final TEFCA will be included in ONC's online TEFCA directory, as directed by the Cures Act. If a Qualified HIN adopts the final TEFCA, is posted in the TEFCA directory, and subsequently decides not to continue participation in the TEFCA, ONC will remove the Qualified HIN from the online TEFCA directory.

For additional information on how ONC intends to work with the RCE, see the User's Guide to Understanding the Trusted Exchange Framework. [20]

[20] See https://www.healthit.gov/sites/default/files/draft-guide.pdf

Comment Process

Interested parties are encouraged to submit comments on any component of the Trusted Exchange Framework, including comments on the feasibility of the principles outlined in Part A – Principles for Trusted Exchange and the language included in Part B – Minimum Required Terms and Conditions for Trusted Exchange to which Qualified HINs would be subject. We also encourage input on the following items:

- Are there particular eligibility requirements for the Recognized Coordinating Entity (RCE) that ONC should consider when developing the Cooperative Agreement?

- Are there standards or technical requirements that ONC should specify for identity proofing and authentication, particularly of individuals?

- We recognize that important health data, such as that included in state Prescription Drug Monitoring Program (PDMPs), may reside outside of EHR/pharmacy systems. In such cases, standards-enabled integration between these systems may be necessary to advance, for example, interstate exchange and data completeness. As such, we invite comment on the following questions:
    - How could a single "on ramp" to data that works regardless of a chosen HIN support broader uses for access and exchange of prescriptions for controlled substances contained in PDMPs?
    - Given the variation of state laws governing PDMP use and data, should interstate connectivity for PDMP data be enabled via a TEFCA use case to address the national opioid epidemic?
    - Is there an existing entity or entities positioned to support the opioid use case directly either as a Qualified HIN within the draft Trusted Exchange Framework or within the proposed Trusted Exchange Framework as a Participant of Qualified HINs? Is there an existing entity or entities positioned to support the opioid use case outside of the draft Trusted Exchange Framework? What is the readiness and feasibility of available standards to support the above and how have they been adopted to date?
    - How could a TEFCA involved approach for supporting opioid use cases distinguish between technical capabilities versus applicable organizational, local, state, and/or federal requirements for PDMPs?

- When a federal agency's mission requires that it disseminate controlled unclassified information (CUI) to non-executive branch entities, but prohibits it from entering into a contractual arrangement, the agency is nevertheless directed to seek the entity's protection of CUI in accordance with Executive Order 13556, Controlled Unclassified Information, or any successor order, and the CUI Program regulations, which include requirements to comply with NIST SP 800-171. How best should TEFCA address these requirements?

How to Submit Comments

The comment period is now open for 45 days. Because of resource limitations, we are only accepting comments electronically at exchangeframework@hhs.gov. Attachments should be in Microsoft Word, Excel, Word Perfect, or Adobe PDF. The deadline for comment submission is 11:59 p.m. E.T. on February 18, 2018.

ONC will review, analyze, and post on our website all public comments that are received by 11:59 p.m. ET on February 18, 2018.[21]

[21] See https://beta.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

Part A – Principles for Trusted Exchange

Purpose & Scope

Part A of the TEFCA provides a set of core principles by which Qualified HINs—as well as all HINs—and data sharing arrangements for data exchange should abide. Specifically, these principles support the ability of stakeholders to access, exchange, and use relevant Electronic Health Information across disparate networks and sharing arrangements. Part B aligns to and builds from these principles to address a minimum set of terms and conditions to enable network-to-network exchange of Electronic Health Information.

Overview of Principles

Part A describes a set of six principles to which all stakeholders should adhere in order to facilitate interoperability and the exchange of Electronic Health Information necessary to support the entire care continuum. The six principles are:

- **Principle 1 - Standardization:** *Adhere to industry and federally recognized standards, policies, best practices, and procedures.*
- **Principle 2 - Transparency:** *Conduct all exchange openly and transparently.*
- **Principle 3 - Cooperation and Non-Discrimination:** *Collaborate with stakeholders across the continuum of care to exchange Electronic Health Information, even when a stakeholder may be a business competitor.*
- **Principle 4 – Privacy, Security, and Patient Safety:** *Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity.*
- **Principle 5 - Access:** *Ensure that Individuals and their authorized caregivers have easy access to their Electronic Health Information.*
- **Principle 6 - Data-driven Accountability:** *Exchange multiple records for a cohort of patients at one time in accordance with Applicable Law to enable identification and trending of data to lower the cost of care and improve the health of the population.*[22]

Each principle is described in detail below and includes lettered sub-principles.

[22] Under the HIPAA Privacy Rule, electronic protected health information (ePHI) can be used or disclosed in various compliant manners such as de-identification or in a limited data set or if the ePHI is disclosed under the "minimum necessary standard." See 45 C.F.R. 164.514.

Principles

Principle 1 - Standardization: Adhere to industry and federally recognized technical standards, policies, best practices, and procedures.

A. **Adhere to standards for Electronic Health Information and interoperability that have been adopted by the Secretary of the U.S. Department of Health & Human Services (HHS) or identified by ONC in the Interoperability Standards Advisory (ISA).**[23]

Qualified HINs and their participants should adhere to federally adopted or recognized standards for Electronic Health Information and interoperability wherever possible, e.g. use of the Consolidated Clinical Data Architecture (C-CDA). Specifically, Qualified HINs should first look to use standards adopted or recognized through ONC's Health IT Certification Program (Certification Program) and in the ISA. If the Certification Program or the ISA do not have applicable standards, Qualified HINs should then consider voluntary consensus or industry standards that are readily available to all stakeholders, thereby supporting robust and widespread adoption. To that end, "proprietary" standards—that is, standards that incorporate or require the use of patented technologies or other intellectual property (IP)—should be avoided unless adequate commitments have been made to license all standards-essential IP pursuant to Reasonable and Non-Discriminatory (RAND) terms.[24] As new standards are adopted by HHS or recognized by ONC, Qualified HINs must implement the updated standards in a timely manner and work with the RCE to update the TEFCA with newer versions of standards as applicable.

In 2015, the Secretary of HHS issued the 2015 Edition Health IT Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications final rule (2015 Edition final rule). [25] The 2015 Edition certification criteria (2015 Edition) help facilitate greater interoperability for several purposes and enables Electronic Health Information exchange through new and enhanced certification criteria, standards, implementation specifications, and Certification Program policies. The 2015 Edition incorporates changes that are designed to spur

---

[23] Under HIPAA, HHS adopted certain standard transactions for the electronic exchange of health care data. These transactions include: Claims and encounter information, Payment and remittance advice, Claims status, Eligibility, Enrollment and disenrollment, Referrals and authorizations; Coordination of benefits, and Premium payment and any of these transactions electronically must use an adopted standard from ASC X12N or NCPDP (for certain pharmacy transactions). The Administrative Simplification provisions under HIPAA and ACA falls under HHS and is carried out by the Division of National Standards (DNS) at CMS and do not apply here. ONC does not have jurisdiction over the standard transactions nor do we advocate any change in these transactions.

[24] See generally, Mark A. Lemley & Carl Shapiro, *A Simple Approach to Setting Reasonable Royalties for Standard-Essential Patents*, Stanford Public Law Working Paper No. 2243026 (November 5, 2013), *available at* http://ssrn.com/abstract=2243026 and http://dx.doi.org/10.2139/ssrn.2243026.

[25] 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications final rule, 80 FR 62601 (Oct 16, 2015) ("2015 Edition final rule").

innovation, open new market opportunities, and provide more choices to stakeholders when it comes to Electronic Health Information exchange.

For example, the 2015 Edition addresses a number of functionality needs related to care delivery, such as the capture of patient information, unique device identifiers for implantable devices, data transport mechanisms, and care plan data. The 2015 Edition also addresses a variety of data exchange flow patterns, including sharing patient data between providers and other health care organizations, between providers and patients, and between providers and public health departments. In addition to the 2015 Edition, ONC has released a Certification Companion Guide[26] for each criterion that further clarifies the certification criteria requirements.

Certification enables End Users to have confidence that their health IT will support interoperability for the appropriate use cases and helps enable the exchange of Electronic Health Information in a structured way. Participants of Qualified HINs that provide services and functionality to providers should follow the 2015 Edition final rule and associated guidance for the certification of health IT where applicable. Further, Qualified HINs that facilitate the exchange of health information should use the standards identified in the 2015 Edition final rule when appropriate for the use case to facilitate connections with other HINs.

As noted above and in addition to the 2015 Edition final rule, the ISA is another resource for standards and implementation specifications. The ISA is a non-regulatory document that coordinates the identification, assessment, and public awareness of interoperability standards and implementation specifications that the industry can use to meet specific clinical health IT interoperability needs. The ISA includes informative characteristics about each standard and implementation specification, including, for example, a rating of standards process maturity (final or balloted draft) and information on implementation maturity (production or pilot).

At a minimum, Qualified HINs connecting to other Qualified HINs should adopt and use standards and implementation specifications that are referenced in the 2015 Edition final rule and the ISA. Further, Qualified HINs should actively engage with ONC to improve and update the ISA's detail, in order to inform the content of the ISA and ensure that the appropriate and best standards are referenced for needed use cases.

B. Implement technology in a manner that makes it easy to use and that allows others to connect to data sources, innovate, and use data to support better, more person-centered care, smarter spending, and healthier people.

Qualified HINs should use standards-based technology for exchanging Electronic Health Information with other Qualified HINs. Such technology should be implemented in accordance with standards and, as consistently as possible, follow implementation guides and authoritative best practices published by

[26] ONC, *Certification Companion Guides, available at* https://www.healthit.gov/policy-researchers-implementers/2015-edition-test-method.

the applicable standards development organization (SDO). Minimizing variation in how standards are implemented will make it easier for others to connect to Electronic Health Information. Further, to the extent possible, Electronic Health Information stored in health IT products should be structured and coded using standardized vocabularies. Qualified HINs and their participants should provide accurate translation and adapter services to their End Users to enable them to map proprietary data to standard, user friendly vocabularies. Adapter services are designed to transform message content or, in this context, transform unstructured data to structured and coded vocabularies, so that Qualified HINs can exchange data with other Qualified HINs in a standardized format.

Qualified HINs should ensure that the data exchanged within their own network and with other Qualified HINs meets minimum quality standards by using testing and onboarding programs to verify minimum quality levels. Qualified HINs may consider using open source tools, such as ONC's C-CDA scorecard tool for testing the quality of C-CDAs.[27] They may also consider developing tools to test the quality of data exchange using Fast Healthcare Interoperability Resources (FHIR) APIs. These types of testing programs can help ensure that high quality data is exchanged both within and across HINs.

Principle 2 - Transparency: Conduct all exchange openly and transparently.

A. Make terms, conditions, and contractual agreements that govern the exchange of Electronic Health Information easily and publicly available.

All parties desiring to participate in Electronic Health Information exchange should know, prior to engaging with a Qualified HIN, the responsibilities of being a participant in a Qualified HIN, the responsibilities of acting as a Qualified HIN, and the protections that have been put in place to ensure that all privacy and security requirements are followed. Qualified HINs should voluntarily make these and other terms and conditions for participating in their network easily and publicly available via their website; meaning they are not accessible only to members but also to the general public.

B. Specify and have all participants agree to the permitted purposes for using or disclosing ePHI or other Electronic Health Information.

Since Qualified HINs are often either Business Associates for Covered Entities or for other Business Associates, their participation agreements specify the permitted purposes for which their network may be used to exchange data. While some Qualified HINs currently support all of the HIPAA permitted purposes, others may only support the Treatment permitted purpose. When Qualified HINs have varying, allowable permitted purposes in their own participation agreements, exchange between those Qualified HINs is limited and may not occur. This could prevent End Users from having a single "on-ramp" to interoperability. Consequently, Part B specifies a minimum set of Permitted Purposes that Qualified HINs and their participants and End Users must support. Qualified HINs may want to support additional permitted purposes and use cases for their participants. If so, they should clearly specify both the minimum set of permitted purposes that are supported and any additional permitted purposes for

[27] ONC, CCDA Scorecard, available at: https://sitenv.org/ccda-smart-scorecard/

using or disclosing Electronic Health Information. These should be specified in the Qualified HIN's legal agreement with Participants, made open and transparent consistent with Principle 2.A, and clearly communicated when Electronic Health Information is requested or sent between Participants and Qualified HINs.

C. Publish, keep current, and make publicly available the Qualified HIN's privacy practices.

HINs and their participants should ascribe to the following privacy practices:

1. Qualified HINs must comply with all Applicable Laws regarding the use and disclosure of ePHI or other Electronic Health Information.
2. Clearly specify the minimum set of "permitted purposes" for using or disclosing ePHI or other identifiable Electronic Health Information within the TEFCA and promote limiting the use of identifiable Electronic Health Information to the minimum amount required for non-treatment purposes. If there are technical variables, the Qualified HINs should clearly specify them.
3. Qualified HINs must have the capability to document and/or capture patient consent or written authorization if required by law and communicate such consent upon request.
4. Qualified HINs must not impede the ability of patients to access and direct their own Electronic Health Information to designated third parties as required by HIPAA.
5. Qualified HINs must have policies and procedures to allow a patient to withdrawal or revoke his or her participation in the exchange of his or her Electronic Health Information on a prospective basis.

These privacy practices are critical to effective exchange and have been incorporated into the terms and conditions in Part B. To further promote transparency, providing public and written notice describing how health information will be used is incorporated into Part B. HIPAA requires that all Covered Entities provide to their patients a Notice of Privacy Practices (NPP). The draft Trusted Exchange Framework requires a participating Covered Entity that is a Qualified HIN to add this information to its existing NPP. The draft Trusted Exchange Framework requires a Qualified HIN that is not a Covered Entity to publish and make available a notice as well.

Principle 3 - Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange Electronic Health Information, even when a stakeholder may be a business competitor.

A. Do not seek to gain competitive advantage by limiting access to individuals' Electronic Health Information.

Qualified HINs and their participants should not treat individuals' Electronic Health Information as an asset that can be restricted in order to obtain or maintain competitive advantage. For example, Qualified HINs and their Participants should not withhold health information requested for TPO purposes from healthcare providers or health plans that are outside of their preferred referral networks or outside of a value-based payment arrangement, such as by establishing internal policies and procedures that use privacy laws or regulations as a pretext for not sharing health information.

Likewise, Covered Entities should not implement technology in a manner that permits limiting the sharing of data. Qualified HINs and their participants should practice data reciprocity (e.g., have a willingness to share Electronic Health Information themselves as opposed to only participating in an exchange relationship only for the purpose of receiving health information from others). In addition, Fees and other costs should be reasonable and should not be used to interfere with, prevent, or materially discourage the access, exchange, or use of Electronic Health Information within a Qualified HIN or between Qualified HINs. Part B further specifies requirements on making any such Fees between Qualified HINs reasonable.

While Qualified HINs must comply with Applicable Laws, including the applicable HIPAA Rules – see OCR's guidance on the HIPAA Security Rule – they should not use contract provisions or proprietary technology implementations to unduly limit connectivity with other Qualified HINs, such as by preventing the appropriate flow of health information across technological, geographic, or organizational boundaries for health and care, safety, quality measurement, payment, or research as permitted by law.

Qualified HIN participants must not prevent the sharing of Electronic Health Information for the permitted purposes specified in Part B because the receiving Covered Entity is considered a competitor. Additionally, Qualified HIN participants may not prevent the sharing of Electronic Health Information for such permitted purposes with a Covered Entity that is not in their preferred referral network or that is not part of an alternative payment model with the Qualified HIN Participant.

Qualified HINs may not use methods that discourage or impede appropriate health information exchange, such as throttling the speed with which data is exchanged, limiting the data elements that are exchanged with healthcare organizations that may be their competitor or a competitor of one of their Participants, or requiring burdensome testing requirements in order to connect and share data with another Qualified HIN.

Principle 4 – Privacy, Security, and Safety: Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity.

A. Ensure that Electronic Health Information is exchanged and used in a manner that promotes patient safety, including consistently and accurately matching Electronic Health Information to an individual.

Ensuring the integrity of electronically exchanged data is paramount to patient safety. When Electronic Health Information is exchanged, the promotion of patient safety begins with correctly matching the data to an individual so that care is provided to the right individual based on the right information. Sophisticated algorithms that use demographic data for matching are the primary method for connecting data to an individual. For example, for purposes of a health IT product seeking certification to the transitions of care criterion of the 2015 Edition, §170.315(b)(1) provides that when Electronic Health Information is exchanged in a C-CDA, a core set of patient demographic data must be included in

a standardized format.[28] Likewise, Qualified HIN participants should ensure that the core set of demographic data is consistently captured for all patients so that it can be exchanged in a standard format and used to accurately match patient data.

In addition to the importance of the integrity of demographic data elements, overall Electronic Health Information integrity is a key component of promoting patient safety in electronic exchange. Where possible, standard nomenclatures should be used and be exchanged in a data format that is consumable by a receiving system, such as the C-CDA or via FHIR Application Programming Interfaces (APIs). Further, Qualified HIN participants need to update individuals' clinical records to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another healthcare organization. Finally, Qualified HINs and their participants should work collaboratively with standards development organizations (SDOs), health systems, and providers to ensure that standards, such as the C-CDA, are implemented in such a way that when Electronic Health Information is exchanged it can be received and accurately rendered by the receiving healthcare organization.

B. Ensure providers and organizations participating in exchange have confidence that the appropriate consent or written authorization was captured, if and when it is needed, prior to the exchange of Electronic Health Information.

The HIPAA Rules do not have a consent requirement for exchanging ePHI for Treatment, Payment, and most Health Care Operations purposes; however, the law does require an authorization from the patient to share ePHI for Health Care Operations purposes with another Covered Entity that does not have a relationship with the patient. Some state and federal laws do require patient consent for exchange of Electronic Health Information. For example, for some health conditions such as HIV, mental health, or genetic testing, state laws generally impose a higher privacy standard (e.g., requiring patient consent from the individual) than HIPAA. Additionally, under 42 C.F.R. Part 2, subject to certain exceptions, federally assisted "Part 2 programs" are required to obtain consent to disclose or re-disclose health information related to substance use disorder information, such as treatment for addiction. When required by federal or state law, a Qualified HIN's ability to appropriately and electronically capture a patients' permission to exchange or use their Electronic Health Information will engender trust amongst other Qualified HINs seeking to exchange with that network. For this reason, we have included this requirement in Part B.

Principle 5 - Access: Ensure that Individuals and their authorized caregivers have easy access to their Electronic Health Information.

A. Do not impede or put in place any unnecessary barriers to the ability of patients to access and direct their Electronic Health Information to designated third parties.

Stakeholders who maintain Electronic Health Information should (1) enable individuals to easily and conveniently access their Electronic Health Information, (2) be able to direct it to any desired location,

[28] See 45 C.F.R. 170.205 for API certification criteria.

and (3) ensure that individuals have a way to learn how their information is shared and used. This principle is consistent with the HIPAA Privacy Rule, which requires Covered Entities to provide PHI to patients in the form and format in which they request it, if it is readily producible in that form and format. This means that if it is stored electronically, patients can request it and access it electronically.

HIPAA also requires Covered Entities and Business Associates to send PHI to a third party of the patient or authorized representative's choosing, upon request. Covered Entities and Business Associates may not impose limitations through internal policies and procedures that unduly burden the patient's right to get a copy or to direct a copy of their health information to a third party of their choosing.[29] Likewise, Qualified HINs and their participants – most of whom are Covered Entities or Business Associates – should not limit third-party applications from accessing individuals' Electronic Health Information via an API when the application complies with Trusted Exchange Framework requirements and is directed by the individual. In addition, Qualified HINs and their Participants should commit to training all staff members on helping individuals obtain electronic access as demonstrated by ONC's access videos and infographic.

Much like individuals' access to their health information as required by HIPAA is important, it also is important for individuals to have access to information about who else has accessed or used their health information. As the Fair Information Practice Principles (FIPPs) of the Nationwide Privacy and Security Framework on openness and transparency states, "[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format."[30] HINs should commit to following this principle, and should provide such opportunities electronically whenever possible, particularly when an individual makes the request electronically. NPP can also serve to help individuals understand how and when their health information is shared.

B. Have policies and procedures in place to allow a patient to withdraw or revoke his or her participation in the Qualified HIN.

Some individuals may prefer not to have their health information electronically shared via a Qualified HIN. Consequently, Qualified HINs and/or their participants must maintain policies and procedures that allow a patient to revoke his/her participation in the Qualified HIN on a prospective basis. Such policies and procedures must be easily and publicly available and be consistent with the HIPAA Privacy Rule right of an individual to request restriction of uses and disclosures, and the process for revoking participation must be easily accomplished by patients.

---

[29] See 45 C.F.R. 164.524

[30] *Nationwide Privacy and Security Framework for Electronic Health Information Exchange of Individually Identifiable Health Information*, http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (December 15, 2008) quoted Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973): http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

Principle 6 - Data-driven Accountability: Exchange multiple records for a cohort of patients at one time in accordance with Applicable Law to enable identification and trending of data to lower the cost of care and improve the health of the population.

A. Enable participants to request and receive multiple patient records, based on a patient panel,[31] at one time.

Health systems and providers may want to use Qualified HINs to decrease the number of discreet interfaces they have to build to exchange Electronic Health Information with other Covered Entities or with their own Business Associates for TPO, Individual Access, Benefits Determination, and Public Health purposes. For example, a provider may want to use a Qualified HIN to share Electronic Health Information from their EHR to a qualified clinical data registry (QCDR), a qualified entity (QE), a health information exchange (HIE), or a health IT developer providing care coordination or quality measurement services. Payers and health plans, including employer sponsored group health plans may wish to work with Qualified HINs to connect to Electronic Health Information that would better support payment and operations, including using analytics for services such as assessing individuals' risk, population health analysis, and quality and cost analysis. These Population Level requests are fundamental to providing institutional accountability for healthcare systems across the country. Additionally, caregivers who are authorized legal representatives, known as "personal representatives" under HIPAA, may wish to access all of their family's records at one time, rather than having to request one record at a time for each family member to the extent permitted by law.

Supporting these types of use cases necessitates the ability to exchange multiple patient records at one time (i.e. population level or "bulk transfer"), rather than potentially performing hundreds of data pulls or pushes for a panel of patients. Qualified HINs should provide the ability for participants to both pull and push population level records in a single transaction. This decreases the amount of time a clinician's resources are devoted to such activity and makes more time available for actual patient care.

[31] A patient panel is a list of patients assigned to a provider, health system, payer, etc.

Part B – Minimum Required Terms and Conditions for Trusted Exchange

Overview

As noted, Congress has charged ONC[32] with ensuring full network-to-network exchange of Electronic Health Information (EHI) through a trusted exchange framework and common agreement (TEFCA). In Part B, we seek to provide a set of minimum, required terms and conditions for the purpose of ensuring that common practices are in place and required of all participants who participate in the final TEFCA. We recognize that all Covered Entities and Business Associates are required to have existing Business Associates' Agreements applicable to the Uses and Disclosures of EHI. The following terms and conditions for trusted exchange align with all the requirements of and sit on the foundation of the HIPAA Rules. These terms and conditions are designed to help ensure, for example:

- Common authentication processes of trusted health information network participants,
- A common set of rules for trusted exchange, and
- A minimum core set of organizational and operational policies to enable the exchange of EHI among networks.

These terms and conditions will be reflected in the Common Agreement and complement the principles and objectives contained in the Principles of Trusted Exchange (Part A). Together Part A and Part B are designed to enable all stakeholders to have a single "on-ramp" to electronic exchange of health information, ultimately easing provider and patient burden.

As with all components of this document, ONC welcomes public comment on the provisions herein.

[32] All capitalized terms or acronyms used herein without definition shall have the respective meanings assigned to such terms in Part B, Section 1 below.

1. Definitions

2015 Edition: the 2015 Edition certification criteria adopted at 45 C.F.R. 170.315.

AALs: the Authentication Assurance Levels described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

Applicable Law: all applicable federal or state laws and regulations then in effect.

Application Programing Interfaces (API): a set of software instructions and standards that allows machine to machine communication.

Attributable Cost: the Reasonable Allowable Cost of the Attributable Services.

Attributable Services refers to both:

(a) the services provided by a Qualified HIN that are necessary for the Qualified HIN to perform its obligations under the Common Agreement to the extent that the Qualified HIN is not providing such services prior to execution of the Common Agreement; and
(b) the services and licenses (if any) that the Qualified HIN must obtain from a third party in order to enter into the Common Agreement and satisfy its obligations thereunder but only to the extent that such third party services and licenses are not already being used in the Qualified HIN's operations prior to entering into the Common Agreement.

Without limitation of the foregoing, Attributable Services include:

(i) the development or modification of APIs for future versions of the USCDI (to the extent that such APIs do not exist prior to execution of the Common Agreement);
(ii) development of or revisions to the Broker in order to satisfy provisions of the Common Agreement that the Qualified HIN's Broker does not satisfy prior to entering into the Common Agreement; and
(iii) the legal services necessary to enter into the Common Agreement and to amend the Qualified HIN's agreements with its Participants in order to meet the requirements of the Common Agreement.

ATNA Integration Profile: the Audit Trail and Node Authentication Integration Profile that is part of the Integrating the Healthcare Enterprise (IHE) International IT Infrastructure Technical Framework.

Benefits Determination: a determination made by any federal or state agency that an individual qualifies for federal or state benefits for any purpose other than healthcare (for example, Social Security disability benefits).

Breach: has the meaning assigned to it in 45 C.F.R. §164.402 of the HIPAA Rules.

Broadcast Query: an electronic method of requesting EHI (sometimes referred to as a "pull") that asks all Qualified HINs and their Participants and End Users if they have EHI of an individual or set of

individuals rather than asking specific Qualified HINs and their Participants and End Users if they have EHI of an individual or a set of individuals.

Broker: see definition of Connectivity Broker below.

Brokered Broadcast Query: a Broadcast Query that (a) uses a Record Locator Service to identify all locations in the Qualified HIN's network (including its Participants and their End Users) that hold an individual's EHI, (b) queries all such locations simultaneously, (c) retrieves all of the individual's EHI from such locations and (d) transmits it back or makes it available to the person or entity that initiated the query. For example, and without limitation of the foregoing, a Broadcast Query that asks for only limited EHI about an individual (such as individual EHI only in certain zip codes) is not a Brokered Broadcast Query unless the limitation was imposed by the person or entity that initiated the Broadcast Query.

Business Associate: has the meaning assigned to such term at 45 C.F.R. §160.103 of the HIPAA Rules.

Common Agreement: the Standard Agreement of the RCE which either (a) initially includes these terms and conditions, or (b) if the RCE has a Standard Agreement prior to the publication of these terms and conditions, its Standard Agreement as modified to include these terms and conditions. The Common Agreement may include such terms from the Standard Agreement or other terms as the RCE and the Qualified HINs deem appropriate; provided, however, that in the event of any conflict or inconsistency between or among Applicable Law, these terms and conditions, the Standard Agreement or any other terms, the following shall be the order of precedence to the extent that there is any conflict or inconsistency: (i) Applicable Law including the HIPAA Rules, (ii) these terms and conditions, (iii) the Standard Agreement, and (iv) any other terms and conditions agreed to by the parties.

Connectivity Broker (Broker): a service provided by a Qualified HIN that provides all of the following functions as further described in these terms and conditions with respect to all Permitted Purposes: master patient index (federated or centralized); Record Locator Service; all types of Queries/Pulls; and EHI return to an authorized requesting Qualified HIN. The Qualified HIN's Broker service must return EHI from across all of the Qualified HIN's Participants and their End Users in a single transaction or, upon request of the initiating Qualified HIN, provide a list of all EHI locations back to the initiating Qualified HIN's Broker and, if further requested by the initiating Qualified HIN, subsequently return the requested EHI to the initiating Qualified HIN.

Covered Entity: has the meaning assigned to such term at 45 C.F.R. §160.103 of the HIPAA Rules.

Current USCDI: the version of the USCDI for which updated APIs and data formats are then required under Section 2.3 below as of the date on which the Query/Pull is initiated.

Data: one or more elements of EHI (unless otherwise expressly specified). If the word data is not capitalized, the foregoing definition shall not apply.

Disclosure: has the meaning assigned in 45 C.F.R. §160.103 of the HIPAA Rules.

Discovery: for purposes of determining the day on which a Breach was discovered, the term discovered shall have the same meaning assigned to it in 45 C.F.R. §164.404 of the HIPAA Rules.

Directed Query: an electronic method of requesting EHI (sometimes referred to as a pull) that asks only specific Participants and/or End Users if they have EHI on an individual or set of individuals.

Electronic Health Information (EHI): any health information regarding an individual that is transmitted by or maintained in electronic media, as defined in 45 C.F.R. 160.103, and includes but is not limited to Electronic Protected Health Information. EHI also includes electronic health data accessed, exchanged or used in the context of the Trusted Exchange Framework and refers to all electronic health-related data developed for an individual, on behalf of an individual or received from an individual that relates to the past, present or future health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual. EHI may, for example, be provided directly from an individual or from technology that the individual has elected to use. It is not required to have been created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university or health care clearinghouse.

Electronic Protected Health Information (ePHI): has the meaning set forth in 45 C.F.R. §160.103 of the HIPAA Rules.

End Entity: a user of public key infrastructure (PKI) digital certificates or an end user system that is the subject of a PKI digital certificate.

End User: an individual or organization using the services of a Participant to send and/or receive EHI.

End User Obligations: all of the obligations of End Users set forth in Section 10 below or elsewhere in these terms and conditions.

FALs: the Federation Assurance Levels described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

Fees: all fees and other amounts charged by a person or entity with respect to the services provided by the person or entity in connection with the Common Agreement. Fees may include but not limited to, one-time membership fees, ongoing membership fees, testing fees, ongoing usage fees, transaction fees, data analytics fees, and any other present or future obligation to pay money or provide any other thing of value.

FIPS PUB 140-2: the Federal Information Processing Standard Publication 140-2, Security Requirements for Cryptographic Modules (May 25, 2001), part of the Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

FHIR: the Fast Healthcare Interoperability Resources specification to the extent formally adopted by HL7.

Health Care Operations : has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules.

Healthcare Provider: has the meaning set forth at 45 C.F.R. §160.103 of the HIPAA Rules.

Health Information Network (HIN): means an individual or entity that --

(a) determines, oversees, or administers policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities;

(b) provides, manages, or controls any technology or service that enables or facilitates the exchange of Electronic Health Information between or among two or more unaffiliated individuals or entities; or

(c) exercises substantial influence or control with respect to the access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities.

HIN Agreement: the written agreement between a Health Information Network and a Participant that uses its services.

HIPAA: the Health Insurance Portability and Accountability Act of 1996 codified at 42 U.S.C. § 300gg, 29 U.S.C § 1181 *et seq.* and 42 USC 1320d *et seq.* and the Health Information Technology for Economic and Clinical Health Act (HITECH) codified at 42 U.S.C. §§ 17921 *et seq.*

HIPAA Rules: as set forth in 45 C.F.R. Parts 160, 162 and 164 and as amended (as applicable) as of the date in question.

HL7: Health Level Seven International, a standards developing organization.

IAL2: Identity Assurance Level 2 described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

IHE: IHE International, Inc., a not for profit corporation (sometimes also referred to as Integrating the Healthcare Environment).

IHE XCA: the cross-community access profile that supports the means to query and retrieve individual relevant medical data held by other communities then most recently formally adopted by IHE.

Individual: Includes the following: an individual as defined by 45 C.F.R. § 160.103, as amended; any other person who is the subject of the electronic health information being accessed, exchanged, or used; a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g), as amended; a person who is a legal representative of and can make health care decisions on behalf of an individual described in this definition; or an executor, administrator or other person having authority to act on behalf of a deceased individual or the individual's estate under State or other law.

Individual Access:

1) With respect to the Permitted Purposes definition, an individual's right to access and obtain a copy of ePHI pursuant to all Applicable Law including, without limitation, 45 C.F.R. §164.524 which sets forth the right of an individual to direct that a copy of ePHI in one or more designated record sets be transmitted to another person designated by the individual. Individual includes a personal representative of the individual in question to the extent permitted under Applicable Law.

2) With respect to a Query/Pull for Individual Access, the response shall be provided as required by these terms and conditions regardless of whether it was initiated for the individual by a consumer or patient-facing application or product selected by the individual that complies with all appropriate privacy and security requirements of this agreement and Applicable Law and is connected to or is itself a Participant or an End User.

Information Blocking: has the meaning set forth in 42 U.S.C. § 300jj–52 and any applicable regulations promulgated thereunder that are then in effect.

ISA: the reference guide version of the Interoperability Standards Advisory then most recently published by ONC on its website or any successor to such document subsequently designated by ONC.

NHIN Authorization Framework 3.0 specification: the specification formally adopted for the Nationwide Health Information Network.

NIST Special Publication 800-63: National Institute of Standards and Technology Special Publication 800-63 (Revision 3), Digital Identity Guidelines.

OASIS: the Organization for the Advancement of Structured Information Standards, a nonprofit consortium.

OAuth 2.0: an authorization framework developed by the Internet Engineering Task Force (IETF) OAuth Work Group.

Onboard: all implementation and other activities necessary for a Participant to become operational in the live environment of a Qualified HIN.

ONC: the Office of the National Coordinator for Health Information Technology of the U.S. Department of Health and Human Services.

OpenID Connect: an interoperable authentication protocol based on the OAuth 2.0 family of specifications promulgated by the OpenID Foundation.

Participant: a person or an entity that participates in a Health Information Network that is a Qualified HIN. Without limitation of the foregoing, a health information exchange could be a Participant with respect to a Qualified HIN.

Participant Agreement: an agreement between a Participant and each of its End Users.

Participant Obligations: all of the obligations of Participants set forth in Section 9 below or elsewhere in these terms and conditions.

Payment: has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules.

Permitted Purposes: Use or Disclosure for Treatment, Payment, Health Care Operations, Public Health, Individual Access, and Benefits Determination as permitted and pursuant to an Authorization and to the extent permitted under Applicable Law.

Population Level: a type of exchange of EHI of multiple individuals in a single transaction, sometimes referred to as a bulk transfer.

Protected Health Information (PHI): has the meaning set forth in 45 C.F.R. §164.501 of the HIPAA Rules.

Public Health: with respect to the definition of Permitted Purposes, a use or disclosure permitted under the HIPAA Rules and any other Applicable Law for public health activities and purposes, including, without limitation, 45 C.F.R. §164.512(b) and 45 C.F.R. §164.514(e) of the HIPAA Rules.

Qualified HIN: a Health Information Network that meets the following criteria and has agreed to the Common Agreement including the terms and conditions set forth herein :

(a) Is an entity that provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand or pursuant to one or more automated processes;
(b) Controls and utilizes a Connectivity Broker service for all EHI exchange subject to the Common Agreement;
(c) Is Participant neutral, meaning that none of the exchanges of EHI by or on behalf of the Qualified HIN include the Qualified HIN itself (whether directly or indirectly) as one of the parties except to the extent that the Qualified HIN receives and maintains such EHI as part of a repository it maintains as a Health Information Network but does not Use or Disclose it except to the extent permitted as a Business Associate under the HIPAA Regulations and other Applicable Law;
(d) Has Participants that are actively exchanging EHI in the data classes included in the then Current USCDI in a live clinical environment in accordance with Section 3 and Section 6 below; and
(e) Demonstrates that it has mechanisms in place, whether by contract or otherwise, (1) to impose all of the Participant Obligations on all Participants who provide or have access to any of the Health Information Network's services; and (2) whether directly or indirectly, to audit Participants' compliance with all relevant obligations and provide for appropriate remedial action (up to and including exclusion) against any Participant that fails to comply with the same.

Query/Pull: includes both Directed Query and any type of Broadcast Query.

Reasonable Allowable Cost: costs of a Qualified HIN that:

(a) were actually incurred;
(b) were reasonably incurred;
(c) are either the direct costs of providing the Attributable Services or are a reasonable allocation of indirect costs of providing the Attributable Services; and
(d) are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

Recognized Coordinating Entity (RCE): the entity selected by ONC that will enter into agreements with HINs that qualify and elect to become Qualified HINs in order to impose, at a minimum, the requirements of the Common Agreement on the Qualified HINs and administer such requirements on an ongoing basis as described herein.

Record Locator Service (RLS): a service that provides the ability to identify where records are located based upon criteria such as an individual's demographic data and/or record data type, as well as providing functionality for the ongoing maintenance of this location information.

SAML (Security Assertion Markup Language): an open standard for exchanging authentication and authorization data between parties, in particular, between an identify provider and a service provider, which has been adopted by OASIS.

SHA-2 (Secure Hash Algorithm 2): a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

SOAP (Simple Object Access Protocol): a protocol specification for exchanging structured information in the implementation of web services in computer networks introduced by several vendors.

SSL (Secure Sockets Layer): a security protocol for establishing encrypted links between a web server and a browser in an online communication, a standard adopted by the Internet Engineering Task Force (IETF).

Standard Agreement: the written agreement between the RCE and a Health Information Network that uses its services.

TEFCA: the Trusted Exchange Framework and Common Agreement then in effect and published in the Federal Register and on ONC's website.

TPO: Treatment, Payment and Health Care Operations.

TLS (Transport Layer Security): a cryptographic protocol that provides communication security over a computer network, a standard adopted by the Internet Engineering Task Force (IETF).

Treatment: has the meaning set forth at 45 C.F.R. §164.501 of the HIPAA Rules.

Use: has the meaning assigned in 45 C.F.R. §160.103 of the HIPAA Rules.

US Core Data for Interoperability (USCDI): As adopted and updated from time to time by HHS, a minimum set of data classes (including, without limitation, specified clinical data fields) that should be exchanged when the data is available.

Whitelist: a list of e-mail addresses or IP addresses from which an application blocking program will allow messages to be received.

XSPA Profile (Cross-Enterprise Security and Privacy Authorization Profile): a profile which has been adopted by OASIS.

XUA Profile (Cross-Enterprise User Assertion Profile): a profile that is part of the IHE International IT Infrastructure Technical Framework.

X.509: a standard for digital certificates promulgated by the International Telecommunication Union (ITU) that uses the international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

2. Requirements of Qualified HINs

2.1 No Limitations on EHI Aggregation. A Qualified HIN shall not limit the aggregation of EHI that is exchanged among Participants, provided that any such EHI aggregation is in support of the Permitted Purposes and in accordance with all Applicable Law.

2.2 Permitted and Future Uses of EHI. Once EHI is shared with another Qualified HIN, the receiving Qualified HIN may exchange, retain, Use and Disclose such EHI only to perform functions in connection with the Permitted Purposes in accordance with the Common Agreement and the Qualified HIN's Participant Agreements or as otherwise permitted by Applicable Law.

2.3 Mandatory Updating of the USCDI. Each Qualified HIN shall update its data format and/or API to include new data classes (including, without limitation, specified clinical data fields) added to the USCDI within a reasonable time (not less than twelve (12) months) after the date of the data classes being officially added to the USCDI.

2.4. Implementation of API. Each Qualified HIN shall implement the APIs necessary to perform its obligations hereunder within twelve (12) months of the date of the API Implementation Guide being formally adopted by HL7 on its public website and recognized by ONC on its public website. For any additional standards necessary for the Qualified HIN's Broker to facilitate interoperable transactions among Qualified HINs, the Qualified HIN shall consult and seek to have its Broker use standards identified in the then most recent ISA.

2.5 Mandatory Updating of Participant Agreements. Each Qualified HIN shall update its Participant Agreements to incorporate the applicable minimum terms and conditions set forth herein within twelve (12) months of the date of the final Common Agreement being published.

2.6 Completion of Onboarding Requirements. Each Qualified HIN shall ensure that each Participant has completed the necessary requirements to Onboard to the Qualified HIN within a reasonable time and is subsequently exchanging EHI in a live environment.

2.7 Compliance with Updated Standards. Except as otherwise expressly provided herein, whenever this Agreement references any standard, implementation specification, or certification criteria to which a Qualified HIN or Participant must comply, the Qualified HIN or Participant shall not be required to comply with any updates to such standards, implementation specifications or certification criteria until twelve (12) months after such standard has been formally adopted by HHS or other applicable authority.

3. Standardization

3.1 Connectivity Broker (Broker) Capabilities: Each Qualified HIN shall provide the following capabilities and take the following actions using its Broker when it: (a) initiates any authorized Query/Pull to another Qualified HIN, or (b) receives an authorized request for EHI from another Qualified HIN (or anyone authorized to act on behalf of a Qualified HIN):

3.1.1 The Broker shall send and receive all of the EHI in the data classes included in the then Current USCDI when and to the extent such EHI is requested and electronically available within or through the Qualified HIN's Health Information Network.

3.1.2 As more fully described in the following provisions of this Section 3, the Qualified HIN's Broker shall send and receive all of the "patient matching data" so labelled and specified in the 2015 Edition certification criterion set forth at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable standards adopted in the future by HHS) when and to the extent that such data is electronically available within or through the Qualified HIN's network to the extent permitted under Applicable Law.

3.1.3 As more fully described in the following provisions of this Section 3, the Qualified HIN's Broker shall adhere to standards and implementation specifications for electronic data and interoperability that are outlined in 45 C.F.R. Part 170, Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS) for the uses to which those standards and implementation specifications are applied. For any additional standards and implementation specifications necessary for the Qualified HIN's Broker to facilitate interoperable transactions among Qualified HINs, the Qualified HIN shall consult and seek to have its Broker use standards and implementation specifications identified in the then most recent ISA.

3.1.4 When a Participant initiates any Query/Pull, (a) the Participant's Qualified HIN shall cause its Broker to initiate the Query/Pull for all EHI in the data classes included in the then Current USCDI to the extent requested and permitted under Applicable Law, and (b) each Qualified HIN shall cause its Broker to respond to all Queries/Pulls for data classes included in the then Current USCDI to the extent requested and permitted under Applicable Law.

3.1.5 Within twelve (12) months after the FHIR standard with respect to Population Level Query/Pulls has been formally approved by HL7, each Qualified HIN shall cause its Broker to be able to initiate and respond to all Query/Pulls for as many individuals as may be requested by another Qualified HIN in a single Query/Pull.

3.1.6 Each Qualified HIN shall cause its Broker to promptly and accurately enter all queries/pulls it initiates or responds to into an audit log and to maintain the audit log as required by Applicable Law.

3.1.7 The Qualified HIN shall cause the Broker to be able to initiate Queries/Pulls and respond to all Queries/Pulls with Brokers of all other Qualified HINs in accordance with both the IHE XCA standards then most recently formally adopted and the certification criterion specified at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS).

3.1.8 Initiating Queries. The Qualified HIN shall cause its Broker to perform the following functions when initiating any Query/Pull:

(a) The initiating Broker of the Qualified HIN shall receive the Query/Pull request from the Qualified HIN's Participants in any format that has been agreed upon within the Qualified HIN's Health Information Network;
(b) The initiating Broker of a Qualified HIN shall send all Queries/Pulls to the Broker of each other Qualified HIN that is then processing Queries/Pulls in a live environment pursuant to the Common Agreement using IHE XCPD or standards specified in the then applicable certification criterion at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS);
(c) Upon receiving confirmation from the responding Broker that an individual's EHI is available, the initiating Broker of the Qualified HIN shall send a Query/Pull to the Broker of each other Qualified HIN that confirmed EHI availability, using IHE XCA or standards specified in the certification criterion at 45 C.F.R. 170 Subpart B as applicable and referenced in the 2015 Edition (or any then applicable standards and implementation specifications adopted in the future by HHS) that would complement or replace a format described herein;
(d) When performing each Query/Pull, the Qualified HIN's Broker shall identify the specific Permitted Purpose for the Query/Pull using a SAML token for the message in accordance with the NHIN Authorization Framework 3.0 specification, Section 3.2.2.6, Purpose of Use Attribute or any successor specification subsequently formally adopted or specified by HHS;
(e) The initiating Qualified HIN shall cause its Broker to consolidate results from all Brokers of other Qualified HINs that respond; and
(f) When delivering responses to an initiating Qualified HIN's own Participant that were received from another Qualified HIN in response to Queries/Pulls from the initiating Qualified HIN's own Participant, the Broker of the initiating Qualified HIN may use any

internally defined interactions (such as individual matching, provider identity, or data transmission) to send EHI to the initiating Qualified HIN's own Participant.

3.1.9 Responding to Queries/Pulls. The Qualified HIN shall cause its Broker to perform the following functions when responding to any Query/Pull from any other Qualified HIN.

(a) The responding Qualified HIN's Broker shall use a Brokered Broadcast Query to determine the Participant and Qualified HIN systems which hold the EHI requested, subject to any limitations set forth in the Query/Pull and to the extent permitted by Applicable Law;
(b) The responding Qualified HIN's Broker may use any internally defined interactions (such as individual matching, provider identity, data transmission) to retrieve all of the EHI in the data classes included in the then Current USCDI from its Participants as long as it responds to the initiating Qualified HIN's Broker in accordance with the other requirements of this Section 3. Additionally, regardless of the format and any problems that may arise from the format in which the Participant entered the EHI or makes it available for a response, the responding Broker is responsible for returning all of the EHI in the data classes included in the then Current USCDI, when and to the extent that such EHI is available and has been requested and the response is in compliance with Applicable Law; and
(c) If more than one Participant internal to the Qualified HIN's Health Information Network has the desired EHI, the responding Broker shall consolidate the results from the multiple Participants into one response to the initiating Broker.

3.2 USCDI

3.2.1 Each Qualified HIN shall exchange all of the EHI in the data classes in the then Current USCDI to the extent such EHI is then available from its Participants and has been requested and to the extent permitted by Applicable Law.

3.2.2 All Participants of a Qualified HIN that collect and maintain EHI in the data classes included in the then Current USCDI, upon request, shall provide all such EHI to fulfill such request to the extent the EHI is available and permitted under Applicable Law.

3.3 Patient Demographic Data for Matching

3.3.1 Each Qualified HIN shall support the exchange of the patient matching data enumerated in the 2015 Edition certification criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) to the extent permitted by Applicable Law.

3.3.2 Participants who collect and maintain the patient matching data enumerated in the 2015 Edition Certification Criterion adopted at 45 C.F.R. §170.315(b)(1)(iii)(G) (or any then applicable certification criteria adopted in the future by HHS) shall provide all such data to the extent permitted by Applicable Law when initiating or responding to Queries/Pulls.

3.4 Data Quality Characteristics

3.4.1 To ensure that Qualified HINs exchange accurate patient demographic data that is used for matching, Qualified HINs shall annually evaluate their patient demographic data management practices using the then current ONC Patient Demographic Data Quality Framework. The first such evaluation shall be conducted within twelve (12) months after the first version of the ONC Patient Demographic Data Quality Framework has been published in final form on ONC's website.

4. Transparency

4.1 Agreements and Fee Schedules

4.1.1 Access to Agreements. Qualified HINs shall make available, respectively, their Standard Agreements and Participant Agreements to ONC and the RCE upon request.

4.1.2 Publication of Fee Schedule. Within fifteen (15) days after signing the Common Agreement, each Qualified HIN shall file with ONC a schedule of Fees used by the Qualified HIN relating to the use of the Qualified HIN's services provided pursuant to the Common Agreement that are charged to other Qualified HINs and/or Participants. If any of the Fees change while the Common Agreement is in effect, the Qualified HIN changing such Fees shall file an updated disclosure of the Fees with ONC within thirty (30) days after the effective date of such change. For purposes of this filing requirement, a change in Fees shall include any change in Fees, waiver of Fees or additional Fees that the Qualified HIN applies to all Qualified HINs and/or Participants or to any one or more of the Qualified HINs or Participants. When filing such fee schedule with ONC, the Qualified HIN shall clearly label all information with respect to Fees that may contain trade secrets or commercial or financial information that is privileged or confidential.

4.2 Publication of USCDI Data Classes. Each Qualified HIN shall publish and maintain on its public website a list of each of the data classes from the then Current USCDI that the Qualified HIN supports for any and all of the Permitted Purposes.

4.3 Disclosures for Patient Safety, Public Health and Quality Improvement Purposes. Upon request, each Qualified HIN shall disclose information to the Participants and other entities described below for the following patient safety, public health, and quality improvement purposes to the extent permitted by Applicable Law: (i) sharing comparative user experiences that may affect patient care; (ii) developing best practices for health information exchange and clinician use; (iii) reporting of EHR-related adverse events, hazards, and other unsafe conditions to government agencies, accrediting bodies, patient safety organizations, or other public or private entities that are specifically engaged in patient quality or safety initiatives; (iv) conducting research studies for peer-reviewed journals; (v) participating in cyber threat sharing activities; and (vi) identifying security flaws in the operation of the Qualified HIN that would not otherwise fall into subsection (v). Participants that are Covered Entities or Business Associates should consider their HIPAA Privacy and Security Rule obligations before sharing EHI for these purposes.

5. Cooperation and Non-Discrimination

5.1 Permitted Purposes and EHI Reciprocity. To the extent permitted by Applicable Law, each Qualified HIN shall support all of the Permitted Purposes by providing, upon request, all of the EHI in the then current USCDI to the extent the EHI is available.

5.2 Non-Discrimination.

5.2.1 A Qualified HIN may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its Participants from joining, exchanging EHI with, conducting other transactions with, using the services of, or supporting any other Qualified HIN.

5.2.2 A Qualified HIN shall not unfairly or unreasonably limit exchange or interoperability with any other Qualified HIN, such as by means of burdensome testing requirements that are applied in a discriminatory manner, sending EHI at different speeds (sometimes referred to as data throttling), or other means that limits the ability of a Qualified HIN to send or receive EHI with another Qualified HIN or slows down the rate at which such EHI is sent or received. As used in this Section 5, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User, or group of them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Qualified HIN because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.

5.2.3 In revising and updating its Broker from time to time, a Qualified HIN will use commercially reasonable efforts to do so in accordance with generally accepted industry practices implemented in a manner that will not cause other Qualified HINs unreasonable cost, expense or delay in executing Queries/Pulls from the revised or updated Broker; provided, however, this provision shall not apply to the extent that such revisions or updates are required by Applicable Law or in order to respond promptly to newly discovered privacy or security threats.

5.2.4 Each Qualified HIN shall use commercially reasonable efforts to provide reasonable prior written notice of all revisions or updates of its Broker to all other Qualified HINs and to the Recognized Coordinating Entity if such revisions or updates could adversely impact the exchange of EHI between Qualified HINs or require changes in the Brokers of any other Qualified HIN regardless of whether they are necessary due to Applicable Law or newly discovered privacy or security threats.

5.3 Fees.

5.3.1 A Qualified HIN must use reasonable and non-discriminatory criteria and methods in creating and applying pricing models if it charges any fees, or imposes any other costs or expenses on another Qualified HIN. Nothing in these terms and conditions requires any Qualified HIN to charge or pay any amounts to another Qualified HIN. Subject to the further limitations set forth below, only the Qualified HIN's Attributable Costs may be charged to another Qualified HIN.

5.3.2 A responding Qualified HIN may charge an initiating Qualified HIN an amount equal to the responding Qualified HIN's Attributable Costs for responding to Queries/Pulls by the initiating Qualified HIN only if they were incurred for the Permitted Purposes of Treatment, Payment, or Health Care Operations. Notwithstanding anything to the contrary set forth in the Common Agreement or elsewhere, a responding Qualified HIN may not charge any amount for responding to Queries/Pulls for the Permitted Purposes of Individual Access, Public Health or Benefits Determination.

5.3.3 A Qualified HIN may not impose any royalty, revenue sharing, or other fee on the use of the EHI (including secondary uses) once it is accessed by another Qualified HIN.

5.4 Broadcast and Directed Queries. Except as required by the HIPAA Rules or other Applicable Law, no Qualified HIN shall enter into any agreement other than the Common Agreement with another Qualified HIN who has also adopted the Common Agreement with respect to any Broadcast Query or Directed Query with respect to any of the Permitted Purposes.

6. Privacy, Security, and Patient Safety

6.1 Privacy Requirements

6.1.1 Individual Access. Each Qualified HIN agrees and acknowledges that individuals have a right to access, share and receive their available ePHI in accordance with the HIPAA Rules, section 4006(b) of the 21st Century Cures Act, and the terms and conditions of the Common Agreement. Each Qualified HIN agrees and acknowledges that individuals have a right to direct a HIPAA Covered Entity to transmit a copy of ePHI in a designated record set to any third parties designated by the individual in accordance with Applicable Law. Similarly, each Qualified HIN agrees and acknowledges that individuals have a right to direct a Participant or End User to transmit a copy of EHI to any third parties designated by the individual in accordance with Applicable Law.

6.1.2 Permitted and Future Uses and Disclosures of ePHI. Once ePHI is shared with another Qualified HIN, the receiving Qualified HIN may exchange, retain, Use and Disclose such ePHI only to perform functions in connection with the Permitted Purposes in accordance with the Common Agreement and the Qualified HIN's Participant Agreements, or as otherwise permitted by Applicable Law.

6.1.3 Breach Notification. When acting as a Business Associate, the Qualified HIN shall comply with all applicable Breach notification requirements regarding ePHI pursuant to 45 CFR §164.410 of the HIPAA Rules. Following discovery of a Breach of ePHI or EHI, the Qualified HIN

further shall notify, in writing, the RCE without unreasonable delay, but no later than fifteen (15) calendar days, after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the RCE shall be responsible for notifying, in writing, other Qualified HINs affected by the Breach within seven (7) calendar days.

6.1.4 Demand for Compulsory Disclosures. If the Qualified HIN is requested or required (by oral questions, interrogatories, requests for information or documents, subpoena, civil investigation, demand or similar process) to disclose any ePHI in connection with a Breach of ePHI, then the Qualified HIN shall provide to the Participant prompt written notice of such request(s), unless such notice is not permitted by Applicable Law, so that the Participant may seek an appropriate protective order and/or waiver of compliance with the provisions of the Common Agreement. In the event that such protective order or other appropriate remedy to prevent such disclosure is not obtained, the Qualified HIN may disclose only that portion of the ePHI (and only to those persons or entities) which is legally required, and the Qualified HIN agrees to reasonably cooperate to the extent permitted by Applicable Law in securing assurances that the disclosed ePHI will be accorded confidential treatment.

6.1.5 Law Enforcement Exception to Breach Notification. If a Qualified HIN is notified, in writing, by any law enforcement official, that a Breach notification would impede a criminal investigation or cause damage to national security, then the Qualified HIN shall delay the Breach notification for the time period specified by the law enforcement official in accordance with the requirements of 45 C.F.R. §164.412 and 45 C.F.R. §164.528(a)(2).

6.1.6 Consent. If and to the extent that Applicable Law requires that an individual's consent to the Use or Disclosure of his or her EHI, the Participant of a Qualified HIN (or the End User of such a Participant) that has a direct relationship with the individual shall be responsible for obtaining and maintaining the consent of the individual (each a "Qualified HIN's Consenting Individual") consistent with the applicable requirements. Each Qualified HIN shall specify such responsibility in its Participant Agreements. Each Qualified HIN shall require its Participants to provide the Qualified HIN with a copy of each consent of a Qualified HIN's consenting individual and the Qualified HIN shall maintain copies of such consents and make them available electronically to any other Qualified HIN upon request.

6.1.7 Revocation of Consent. Consistent with Applicable Law, each Qualified HIN agrees to maintain policies and procedures to allow an individual to withdraw or revoke his or her permission for the Use and Disclosure of the individual's EHI as obtained under Section 6.1.6 on a prospective basis.

6.1.8 Written Notice. Each Qualified HIN agrees to publish and make publicly available a written notice in plain language that describes each Qualified HIN's privacy practices regarding the access, exchange, Use and Disclosure of ePHI with substantially the same content as described in 45 CFR §164.520(b). The written notice must contain a description, including at

least one (1) example of each type of Permitted Purpose. If a Qualified HIN is a Covered Entity, the Qualified HIN's Notice of Privacy Practices must meet the requirements of 45 CFR §164.520.

6.2. Minimum Security Requirements. To ensure the confidentiality, integrity, and availability of ePHI and consistent with the Security Rule, each Qualified HIN (a Business Associate under the HIPAA Rules) shall be required to implement the following minimum security requirements described below within twelve (12) months from the date the TEFCA is published in the Federal Register, unless otherwise specified below. As a Business Associate, each Qualified HIN acknowledges that it is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making Uses and Disclosures of ePHI that are not authorized by its contract or required by Applicable Law. Each Qualified HIN further acknowledges that a Business Associate is directly liable and subject to civil penalties for failing to safeguard ePHI in accordance with the HIPAA Security Rule.

6.2.1 HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework (CSF). In addition to complying with the HIPAA Security Rule and the 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, each Qualified HIN shall evaluate its security program on at least an annual basis. As part of its ongoing security risk analysis and risk management program, this evaluation must include a review of the NIST CSF HIPAA Security Rule Mapping, the ONC/OCR HIPAA Security Risk Assessment Tool, and the ONC Guide to Privacy and Security of Electronic Health Information, as tools to help ensure its compliance with the HIPAA Rules and to improve its ability to secure ePHI and other critical information and business processes. To the extent that a review of the NIST CSF HIPAA Security Rule Mapping identifies any gaps in the Qualified HIN's compliance with the HIPAA Rules or other Applicable Law, then the Qualified HIN shall assess and implement evolving technologies and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits, and provide documentation of such evaluation.

6.2.2 Data Integrity. Each Qualified HIN's security policy shall include the following elements to ensure data integrity of all EHI that it receives, maintains or transmits:

(i) Procedures to ensure that EHI is not improperly altered or destroyed;

(ii) Procedures to protect against reasonably anticipated, impermissible uses or disclosures of EHI;

(iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the Qualified HIN is serving as a certificate authority; and

(iv) Procedures to test and restore backup copies of systems, databases, and private keys, if the Qualified HIN is serving as a certificate authority, to ensure each Qualified HIN can

retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve data integrity.

Each Qualified HIN shall report instances of inaccurate or incomplete EHI to the Participant who is the originator of the EHI, and request that Participant remediate such data integrity issues in a timely manner to the extent reasonably possible.

6.2.3 Access Control – Authorization. Each Qualified HIN's security policy shall include the following elements to ensure appropriate access controls and user authentication:

(i) Procedures to ensure that users attempting to access system functions and EHI possess the appropriate credentials (such as privileges granted and provisioned in security and privacy management) to access the minimum necessary information needed;

(ii) For SOAP-based transactions, the implementation of the OASIS XSPA Profile of SAML;

(iii) For SOAP-based transactions, the implementation of the OASIS XSPA Profile of extensible Access Control Markup Language (XACML) Profile for authenticating, administering, and enforcing authorization policies that control access to health information residing within or across enterprise boundaries; and

(iv) For FHIR APIs-based transactions, the SMART App Authorization Guide for the use of OAUTH 2.0.

6.2.4 Identity Proofing. Each Qualified HIN's security policy shall include the following elements to ensure appropriate identity proofing:

(i) End Users/Participants. Each Qualified HIN shall identity proof Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials; and

(ii) Individuals. Each Qualified HIN shall identity proof individuals at a minimum of IAL2 prior to issuance of credentials; provided, however, that the Qualified HIN may supplement identity information by allowing Participant staff to act as trusted referees. Participant staff also may act as authoritative sources by using knowledge of the identity of the individuals (*e.g.*, physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All personally identifiable information collected by the Participant staff or Qualified HIN shall be limited to the minimum necessary to resolve a unique identity.

6.2.5 Authentication.

(i) Individuals. Each Qualified HIN shall authenticate individuals at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

(ii) End Users/Participants. Each Qualified HIN shall authenticate End Users and Participants at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

(iii) For FHIR API-based transactions the SMART App Authorization Guide for the use of OAUTH 2.0.

(iv) For FHIR API-based transactions that require End User authentication, the identity data scopes of the SMART App Authorization Guide for the use of OpenID Connect 2.0.

6.2.6 Credential Management. Each Qualified HIN's security policy shall include the following elements to ensure appropriate credential management:

(i) Each Qualified HIN's issuer certificate authorities and registration authorities shall protect repository information not intended for public dissemination or modification. Each Qualified HIN issuer certificate authorities shall provide unrestricted read access to the Qualified HIN's repositories for legitimate uses and shall implement logical and physical access controls to prevent unauthorized write access to such repositories.

6.2.7 Transport Security. Each Qualified HIN's security policy shall include the following elements to ensure appropriate data transport security:

(i) Authentication Server Requirements.

(a) SOAP-based Security. Each Qualified HIN's SOAP-based servers shall conform to the connection authentication requirements as specified in the IHE ATNA Integration Profile for Transport Authentication Security. Each Qualified HIN using local authentication or federated authentication for SOAP-based requests shall convey the locally-authenticated user attributes and authorizations using SAML 2.0 assertions as detailed in the IHE XUA Profile.

(b) At a minimum, Qualified HINS shall employ the following ciphers to mitigate the risk of EHI being exposed during transport in order to eliminate all readable EHI that is not encrypted:

- Null cipher where encryption is not necessary, but must be configured for the system to work;
- Substitution cipher as a minimum cryptographic technique to render EHI unreadable; and
- Transposition ciphers or other more advanced cipher techniques to render unsecured EHI information unusable, unreadable or indecipherable to unauthorized individuals.

(c) Each Qualified HIN shall ensure that message exchanges are secured using TLS/SSL 1.2 X.509 v3 certificates for authentication, and X.509 certificates are used for authentication of all transactions.

(d) FHIR APIs. Each Qualified HIN shall require Participants to conform to the recommendations described in both the Security Considerations sections of RFC 6749 and in the OAuth 2.0 Threat Model and Security Considerations sections of RFC 6819.

(ii) Authentication Server Requirements for Third Party Application Access. Each Qualified HIN's security policy that supports third party application access shall implement the following requirements within three (3) months from the date that the Qualified HIN executes an agreement with the RCE; provided, that if the Qualified HIN has not currently implemented FHIR, then the Qualified HIN shall implement the following requirements within twelve (12) months from the date that the Qualified HIN executes an agreement with the RCE:

(a) Each Qualified HIN shall support the OAuth 2.0 Dynamic Client Registration Protocol for Individual registration as defined in RFC 7591; and

(b) Each Qualified HIN shall authenticate third party applications to the authorization server's endpoint using a JSON Web Token (JWT) assertion signed by the third party application's private key as defined in RFC 7519.

(iii) Authorization Server Requirements. Each Qualified HIN's security policy shall implement the following authorization server requirements within twelve (12) months of the API Implementation Guide being published as specified in Section 2.4 above:

(a) Each Qualified HIN's authorization server shall compare a Participant's registered redirect universal record indicators with the redirect universal record indicators presented during an authorization request using an exact string match to avoid spoofing;

(b) Each Qualified HIN shall ensure that its authorization servers maintain access tokens to single use for a short lifetime of less than ten (10) minutes;

(c) Each Qualified HIN shall ensure that its authorization servers use refresh tokens for long term access to the user information endpoint or other similar protected resources; and

(d) Each Qualified HIN shall ensure that its authorization servers shall provide a mechanism for the End User to revoke access tokens and refresh tokens granted to a Participant or individual.

6.2.8 Certificate Policies. Each Qualified HIN's security policy shall include the following elements to ensure that all Participant SSL certificates meet or exceed the following criteria:

(i) Key Sizes:

- The certificate authority shall utilize the SHA-256 algorithm for certificate signatures; and
- All keys shall be at least 2048 bit.

(ii) Certificate Authority:

- The certificate authority's certificate shall be issued by a mutually trusted certificate authority; and
- The certificate authority's certification shall not be self-signed.

6.2.9 Policy Binding. Each Qualified HIN's security policy shall include the following elements to ensure appropriate policy binding by associating the X.509 digital certificate to the trust domain by meeting the following conditions:

(i) The End Entity certificate possesses a subject distinguished name attribute with a single common name component equal to the fully qualified domain name of the Listed End Point;

(ii) The End Entity certificate possesses a subject distinguished name attribute with an organizational unit component representing the trust domain name;

(iii) The End Entity certificate has at least one (1) subject alternative name extension type of universal record indicator and value representing the trust domain name; and

(iv) An approved trust chain issues the End Entity certificate.

6.2.10 Auditable Events. Each Qualified HIN shall publicly log the existence of TLS/SSL certificates as they are issued or observed in a manner that permits an audit of the certificate authority. Additionally, each Qualified HIN shall audit the certificate logs to identify the issuance of any suspect certificates. For certificate transparency purposes, each Qualified HIN that acts as a certificate authority shall maintain certificate logs on an ongoing basis. Each certificate log must publicly advertise its URL and its public key via HTTPS GET and POST messages. Each Qualified HIN that acts as a certificate authority shall refuse to honor certificates that do not appear in a certificate log. Each Qualified HIN's security policy shall include the following elements to ensure appropriate auditing:

(i) Each Qualified HIN shall generate audit log files for all events. Each Qualified HIN further shall retain all security audit logs (both electronic and non-electronic) and make such audit logs available during any audits. At a minimum, each audit record shall include the following information (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;

- A success or failure indicator; and (where appropriate)
- The identity of the entity and/or operator that was responsible for the event.

6.2.11 Cryptography. Each Qualified HIN shall use asymmetric (*e.g.*, public-key) ciphers for generating secret keys, establishing long-term security credentials and providing non-repudiation services. Each Qualified HIN further shall ensure mutual handshake exchange is based on cryptographic techniques (*e.g.*, TLS 1.2 or above). In addition, members of the trust framework shall deploy a validated cryptographic subsystem consistent with the requirements described in FIPS PUB 140-2. Each Qualified HIN shall ensure that cryptographic modules are validated to the FIPS PUB 140-2 minimum level for the relevant party (or an equivalent protection). Additionally, each Qualified HIN shall apply end-user device encryption standards as adopted in the 2015 Edition final rule. (See §170.314(d)(7)).

6.2.12 IP Whitelist. Each Qualified HIN shall publish and share all IP addresses that are whitelisted. An IP Whitelist can be implemented by the Qualified HIN's end point only if the result complies with the applicable Qualified HIN Participant's non-discrimination policy. For the purposes of this subsection, an end point will be the web service technical URL hosted by a Qualified HIN that is listed in the online TEFCA directory.

6.2.13 Incident Response. Each Qualified HIN who is an issuer of certificate authorities shall maintain backup copies of system, databases, and private keys in order to rebuild the certificate authorities' capability in the event of software and/or data corruption.

7. Access

7.1 Obligation to Respond to Queries/Pulls. Each Qualified HIN shall respond to all Queries/Pulls by providing all of the EHI in the data classes in the then Current USCDI when and to the extent available, requested and permitted by Applicable Law for the Permitted Purpose of Individual Access, provided that the requesting Qualified HIN has adhered to the privacy and security requirements outlined in Section 6. Notwithstanding the foregoing, a Qualified HIN shall not be required to include individuals as Participants or End Users.

7.2 Individual Requests for No Data Exchange. Each Qualified HIN shall provide a method for individuals who do not wish to have their EHI exchanged and post instructions on its public website for both recording and communicating such requests to the Qualified HIN at no charge to the individuals. Each Qualified HIN shall process all requests from individuals or from Participants on behalf of individuals in a timely manner and ensure that such requests are honored by all other Qualified HINs on a prospective basis. As a HIPAA Business Associate, the Qualified HIN must also enable a Covered Entity to process the request consistent with the right of an individual to request restriction of Uses and Disclosures.

8. Data-driven Choice

8.1 Population Level Data

8.1.1 Query/Pull: Within twelve (12) months of the standard referenced in 4.1.5 being formally adopted by HL7, the Qualified HIN's Broker shall be able to exchange EHI regarding as many individuals as satisfy the search parameters or are otherwise specified by any requesting Qualified HIN in response to a single Query/Pull.

8.1.2 A Qualified HIN may limit responses to Population Level EHI Queries/Pulls to specific time periods to minimize system disruption due to a lack of bandwidth provided that such limitations are reasonable and do not extend for more than a twenty-four (24) hour period.

8.1.3 Each Qualified HIN must support Population Level EHI Queries/Pulls as described above for all of the Permitted Purposes in accordance with Applicable Law.

9. Participant Obligations

9.1 Each Qualified HIN shall be responsible for ensuring that the obligations described in this Section 9 shall be incorporated into all existing and future Participant Agreements.

9.1.1 Permitted Purposes. Each Participant shall support all of the Permitted Purposes by providing all of the data classes the then current USCDI when and to the extent available when requested and permitted by Applicable Law. Each Participant shall respond to Queries/Pulls for the Permitted Purposes.

9.1.2 Non-Discrimination.

(i) A Participant may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its End Users from joining, exchanging data with, conducting other transactions with, using the services of or supporting any other Participant.

(ii) A Participant shall not unfairly or unreasonably limit exchange or interoperability with any other Qualified HIN or Participant via burdensome testing requirements that are applied in a discriminatory manner, data throttling, or any other means that limits a Qualified HIN or Participant from sending and receiving health information with another Qualified HIN or slows down the rate at which such data is sent or received. As used in this Section 9, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User or group of them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Qualified HIN or Participant because it primarily serves providers that are not users of a certain electronic health

record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.

9.1.3 Privacy. Each Participant agrees to comply with all applicable federal and state laws and regulations relating the privacy of health information.

9.1.4 Identity Proofing. Each Participant shall identity proof participating End Users and individuals in accordance with the following requirements:

(i) End Users. Each Participant shall identity proof participating End Users at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; and

(ii) Individuals. Each Participant shall identity proof individuals at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; provided, however, that the Participant may supplement identity information by allowing its staff to act as trusted referees and authoritative sources by using personal knowledge of the identity of the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All collected personally identifiable information collected by the Participant shall be limited to the minimum necessary to resolve a unique identity and the Participant shall not copy and retain such personally identifiable information.

9.1.5 Authentication. Each Participant shall authenticate participating End Users and individuals in accordance with the following requirements:

(i) Individuals. Each Participant shall authenticate participating individuals at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

(ii) End Users. Each Participant shall authenticate End Users at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

9.1.6 Security Incident and Breach Notification Requirements. Each Participant who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each Participant further shall notify, in writing, the Qualified HIN without unreasonable delay, but no later than fifteen (15) calendar days after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the Qualified HIN shall be responsible for notifying, in writing, other Participants affected by the Breach within seven (7) calendar days.

9.1.7 Security Technical Requirements. Each Participant shall be responsible for complying with the technical security policy requirements relating to authentication, identity proofing and individual authorization described in Sections 6.2.3 to 6.2.5.

9.1.8 Exchange of Data Elements. Each Participant shall be responsible for exchanging data elements, if available, in accordance with the USCDI and patient demographic data for matching enumerated in Sections 3.2.2, 3.3 and 3.4.

9.1.9 Compliance with Applicable Law. Each Participant shall comply with all applicable federal and state laws and regulations.

9.2 Participant Compliance. Each Qualified HIN shall be responsible for taking reasonable steps to ensure that all Participants are abiding by the obligations stated in this Section. Each Qualified HIN further shall require that each Participant provide written documentation evidencing compliance with these obligations on at least an annual basis. In the event that a Qualified HIN becomes aware of a Participant's non-compliance with any of the obligations stated in this Section, then the Qualified HIN immediately shall notify the Participant in writing and such notice shall inform the Participant that its failure to correct any deficiencies may result in the Participant's removal from the Health Information Network.

9.3 Failure to Comply with Common Agreement. Each Qualified HIN, each Participant of a Qualified HIN, and each End User acknowledges that the Recognized Coordinating Entity, other Qualified HINs, other Participants, and other End Users may report any failure to incorporate or to abide by the terms and conditions of the Common Agreement to ONC and/or the Office of the Inspector General, if the Qualified HIN, Participant, or End User has a reasonable belief that the conduct may constitute information blocking (as defined by Section 3022(a)(1) of the Public Health Services Act) or, with respect to a health IT developer, that the conduct is contrary to any condition or requirement of the developer's certification under any program(s) maintained or recognized by ONC. A Qualified HIN's failure to incorporate the Common Agreement's terms and conditions into a Participant Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.

9.4 Incorporation of Participant Obligations. Each Participant shall ensure that the obligations described in this Section 9 are incorporated into all existing and future agreements with the entities and individuals with which it exchanges information.

9.5 Compliance with Emergency Preparedness Requirements. Each Qualified HIN and each Participant shall comply with the *Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers as further described in* 81 FR 63859.

10. End User Obligations

10.1 Each Participant shall be responsible for ensuring that the obligations described in this Section 10 shall be incorporated into all existing and future End User Agreements.

10.1.1 Permitted Purposes. Each End User shall support all of the Permitted Purposes by providing all of the data classes of the then current USCDI to the extent available when requested and permitted by Applicable Law. Each End User shall respond to Queries/Pulls for the Permitted Purposes.

10.1.2 Non-Discrimination. An End User shall not unfairly or unreasonably limit exchange or interoperability with any Participant such as by means of burdensome testing requirements that are applied in a discriminatory manner, data throttling, or any other means that limits the ability of a Qualified HIN or Participant to send or receive EHI with another Qualified HIN or slows down the rate at which such data is sent or received. As used in this Section 10, a discriminatory manner means action that is taken or not taken with respect to any Qualified HIN, Participant or End User or group of them due to the role it plays in the healthcare system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that different treatment shall not be deemed discriminatory to the extent that it is based on a reasonable belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Participant or End User because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.

10.1.3 Identity Proofing. Prior to the issuance of access credentials by Participant, each End User shall be required to identify proof at Identity Assurance Level 2 (IAL2).

10.1.4 Authentication. Prior to the issuance of access credentials by Participant, each End User shall be required to authenticate at AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

10.1.5 Security Incident and Breach Notification Requirements. Each End User who is a Covered Entity or Business Associate shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Rules. Each End User further shall notify, in writing, the Participant, if affected by the Breach, without unreasonable delay, but no later than fifteen (15) calendar days after discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations.

10.1.6 Exchange of Data Elements. Each End User shall be responsible for exchanging data elements, if available, in accordance with the USCDI and patient demographic data for matching enumerated in Section 3.2.2, 3.3 and 3.4.

10.1.7 Failure to Comply with Common Agreement. Each Qualified HIN, each Participant of a Qualified HIN, and each End User acknowledges that the Recognized Coordinating Entity, other Qualified HINs, other Participants, and other End Users may report any failure to incorporate or to abide by the terms and conditions of the Common Agreement to ONC and/or the Office of the Inspector General, if the Qualified HIN, Participant, or End User has a reasonable belief that the conduct may constitute information blocking (as defined by Section 3022(a)(1) of the Public Health Services Act) or, with respect to a health IT developer, that the conduct is contrary to any condition or requirement of the developer's certification under any program(s) maintained or recognized by ONC. A Participant's failure to incorporate the Common Agreement's terms and

conditions into an End User Agreement to the extent required herein shall be considered evidence of a material breach of the Common Agreement.

10.1.8 Compliance with Applicable Law. Each End User shall comply with all applicable federal and state laws and regulations.

Attachment 8

CYBERSECURITY BILLS SIDE-BY-SIDE

BILL	SPONSORS	COMMITTEE	SUMMARY
S. 1961 – Internet of Things Cybersecurity Improvement Act of 2017	Warner (D-VA), Gardner (R-CO)	Senate Homeland Security and Government Affairs	To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.
S. 1656 – Medical Device Cybersecurity Act of 2017	Blumenthal (D-CT)	Senate HELP	To amend the Federal Food, Drug, and Cosmetic Act to provide cybersecurity protections for medical devices.
H.R. 3985 – Internet of Medical Things Resilience Partnership Act	Brooks (R-IN), Trott (R-MI)	House Energy and Commerce	To establish a working group of public and private entities led by the Food and Drug Administration to recommend voluntary frameworks and guidelines to increase the security and resilience of Internet of Medical Things devices, and for other purposes. Not later than 5 months after the date of enactment of this Act, the Commissioner of the Food and Drug Administration, in consultation with the National Institute of Standards and Technology, shall establish a working group of public and private entities to develop recommendations for voluntary frameworks and guidelines to increase the

CYBERSECURITY BILLS SIDE-BY-SIDE

			security and resilience of networked medical devices sold in the United States that store, receive, access, or transmit information to an external recipient or system for which unauthorized access, modification, misuse, or denial of use may result in patient harm.
H.R. 4191 – HHS Cybersecurity Modernization Act	Long (R-MO), Matsui (D-CA)	House Energy and Commerce	To amend the Public Health Service Act to authorize the Secretary of Health and Human Services to designate an officer within the Department of Health and Human Services as having primary responsibility for the information security (including cybersecurity) programs of the Department, and for other purposes.
Varian proposal	TBD	TBD	HIPAA safe harbor for accredited persons

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Date: January 9, 2018

To: Healthcare Association Stakeholders (*recipients at bottom*)

From: Healthcare Sector Coordinating Council Cybersecurity Working Group (CWG) Co-Chairs:
Terry Rice, Merck
Bryan Cline, HITRUST

Cc: Greg Garcia, HSCC CWG Executive Director

Subject: **February 6 Healthcare Sector Coordinating Council Cyber Working Group DC Meeting**

This is a call to action to the healthcare sector to coalesce around the urgency of protecting our information and operational infrastructures against cyber threats.

Each of your associations represents a critical subsector of the healthcare industry, and each is part of an interdependent ecosystem that is facing increasingly sophisticated cybersecurity threats and vulnerabilities that can cascade across the value chain of the healthcare sector, ultimately affecting patient safety, security and privacy. We know you will agree it is our collective responsibility to deliver industry-wide policy and operational solutions to this shared challenge.

Our responsibility. This responsibility is captured in three iterations of a Presidential Executive Order dating to 1998, the most recent being Presidential Policy Directive 21 in 2013, which calls on 16 critical industry sectors to self-organize – in partnership with the government - around the mission to protect essential assets and services from existential threats. Every critical industry sector, including healthcare, financial services, electricity, emergency services, communications, water, transportation, and others, has been stepping up to this mission. We do this with two essential functions: the day-to-day operational protection, threat analysis and incident response of the National Health Information Sharing and Analysis Center (NH-ISAC), and the longer-term strategic and policy-oriented mission of the Healthcare Sector Coordinating Council (HSCC).

What is the HSCC and what does it do? We have had discussions with many of you about the HSCC – recognized under the Executive Order as the private industry partner to the Department of Health and Human Services. The HSCC is in effect an association of associations, which also must include your members, convening at the HSCC "big table" to identify and attack those cross cutting threats and vulnerabilities that challenge our ability to deliver safe and secure healthcare to the nation. We do this both independent of, and in partnership with, the Department of Health and Human Services – our "sector specific agency." During designated working sessions between government and industry, competitive and regulatory equities are left outside the door, and sensitive information discussed with the government is *afforded protection from public disclosure under special advisory committee status*.

While every association member participating in the HSCC maintains its own business-as-usual programs, the HSCC gives your organization visibility into other subsector perspectives and work initiatives, and a process-driven coordination mechanism to minimize conflict or duplication. **There are no membership dues to participate in the HSCC – only the contribution of your organization's available expertise, governance process, and programmatic**

reach in the development and implementation of policy and operational improvements to the security and resiliency of the sector.

The HSCC Cybersecurity Working Group. Over the past year, one component of the HSCC – the **Cybersecurity Working Group (CWG)** - has undertaken a number of important cybersecurity initiatives. Additional workstreams are expected to get underway for medical device and health IT security strategy and, more broadly, implementation of the Healthcare Industry Cybersecurity Task Force Report recommendations released in June 2017.

Call to Action. **The purpose of this message is a call to action to you and your membership.** As co-chairs of the HSCC Cyber Working Group, we observe that the sector's cybersecurity mission should be more robustly represented – both numerically and substantively -- across the six major subsectors: Direct Patient Care; Health Information Technology; Health Plans & Payers; Labs, Blood & Pharmaceuticals, Mass Fatality Management Services; and Medical Materials. Accordingly, we urge you to ensure that your organizations - representing critical service and technology providers with extensive economic concentration and population reach - are at the CWG table, providing expertise and resources to collaboratively address complex cybersecurity problems, and to partner with our government stakeholders in that process. We must operate under the principle that none of us individually is as smart as all of us collectively.

Hippocrates Initiative. We are now launching "Hippocrates" – our HSCC Cybersecurity Working Group acceleration initiative. As the father of modern medicine, Hippocrates did more than say "First, do no harm." He approached medicine with a rigorous, evidence-based discipline of diagnosis and care. This is the same method that drives our council work, and the malady is our collective "cyber insecurity" and its ultimate threat to patient safety, security and privacy.

Mark your calendars. Thus, ***we are calling an organizing meeting of the Healthcare Sector Council's Hippocrates Initiative for February 6, 2018 from 8:30am – 1:00pm*** (including a working lunch), and we strongly encourage you to attend and bring your horsepower. ***The meeting will be held at the U.S. Access Board, 1331 F Street, NW, downtown DC***. There, we will kick off Hippocrates with the following objectives:

- Convene national-level associations to significantly enhance membership numbers and representation at the HSCC CWG table
- Commit your associations' governing structures and member leadership to recruit the most influential and knowledgeable executives and subject matter experts to CWG liaison and leadership support. You must come to the table with your members' mindshare and authority to speak on their behalf according to your protocols
- Agree to a transparent and representational governance structure for the HSCC Cyber Working Group; and
- Coalesce around high-level cybersecurity and resilience principles around which we will organize task groups to accomplish collectively-prioritized objectives with measurable deliverables and outcomes

Then we will assemble the teams, elect our leaders and deliver what is expected of us – a more secure and healthier nation.

Who should attend. You can contribute any combination of skill sets to the Cyber Working Group including:

- CIO's, CISOs and their specialists
- Information and operational technology
- Legal counsel
- Government relations, and
- Risk and compliance.

Senior government officials to affirm the partnership. We will have with us at the start of this organizing meeting the HHS Assistant Secretary for Preparedness and Response, Robert Kadlec, and the Department of Homeland Security Assistant Secretary for Cybersecurity and Communications, Jeanette Manfra, to congratulate us on our renewed commitment and challenge us to deliver on our collective responsibility. They will then leave us to organize and work through our priorities and build the team.

We will send out to you shortly a calendar invitation, and more information about the agenda and expectations will follow. It is essential that your association and members are represented, and that you come prepared to take ownership of this responsibility and your leadership in it.

Attached is a powerpoint FAQ for additional background. Please direct questions to Executive Director Greg Garcia (greg.garcia@HealthSectorCouncil.org).

Who is invited so far. The table below lists 40 organizations so far receiving this invitation. We know there are many national associations with whom we have yet to reach out to, so we encourage you to make recommendations or introductions for such additions to Greg Garcia. After this organizational meeting we will work with you to launch successive rounds of membership development to recruit essential stakeholders across your association memberships.

Advanced Medical Technology Association	Aetna/NH-ISAC	Alliance for Nursing Informatics	America's Health Insurance Plans
American Association of Nurse Practitioners	American Health Care Association	American Health Information Management Association	American Hospital Association
American Medical Association	American Medical Group Association	American Medical Informatics Association	Association for Executives in Healthcare Information Security
Association for Healthcare Resource and Materials Management	Association for the Advancement of Medical Instrumentation	Biotechnology Innovation Organization	Blue Cross Blue Shield Association (BCBSA)
Center for Medical Interoperability	College of American Pathologists	College of Healthcare Information Management Executives	Cooperative Exchange/National Clearinghouse Association
Electronic Healthcare Network Accreditation Commission	Federation of American Hospitals	Healthcare Administrative Technology Association	Healthcare Industry Distributors Association
Healthcare Information & Management Systems Society	Healthcare Leadership Council	Healthcare Ready	HITRUST
Hospital Corporation of America	Medical Device Information Sharing and Analysis Organization	Medical Device Innovation Consortium	Medical Device Innovation Safety & Security Consortium
Medical Device Manufacturers Association	Medical Group Management Association	Medical Imaging Technology Association	National Association of Chain Drug Stores
NH-ISAC	PhRMA	Univ. Chicago Hospitals	Workgroup for Electronic Data Interchange

Attachment 10

Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HPH SCC
CYBERSECURITY WORKING GROUP

A PRIMER

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

What Is It?

- The cross-sector coordinating body representing one of 16 critical infrastructure sectors identified in Presidential Executive Order (PPD-21)
- A trust-community partnership convening companies, non-profits and industry associations across six subsectors with HHS, DHS, law enforcement, and intelligence community
- ***Mission: to identify cyber and physical risks to the security and resiliency of the sector, and develop planning guidance in a 3-year Sector Specific Plan and implementing task groups for mitigating those risks***
- In meeting with government, it is the "Healthcare & Public Health SCC (HPH SCC")
- Focused on longer-term critical infrastructure policy and strategy, complementing the operational National Health Information Sharing and Analysis Center, which serves as the sector's tactical watch, warning, incident response, forensics, and best practices hub for intra-sector and government information sharing

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

How Does It Operate?

- Serves as a coordinating body – "the big table"- for industry associations and their members to unify effort toward policy and strategic solutions to shared security and resiliency challenges
- Does *not* supplant association work but coordinates their visibility, prioritization, and deconfliction
- Organized along functional and policy working groups with specific deliverables
- Regular meetings and conference calls and ongoing interaction with HHS as the principal sector specific agency (SSA)
- Forges joint work products – separately and with the government - that can be implemented across the sector to improve security and resiliency
- Strives to address *cross-cutting* issues affecting two or more subsectors, requiring industry associations and members to use their governing structures to enable accurate representation of their positions and agree to joint initiatives and outcomes

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

Who Is In It?

- The HSCC is composed of major stakeholders from the six HHS-identified sub-sectors - industry associations and their member organizations & individuals:
  - Direct Patient Care
  - Health Information and Medical Technology
  - Health Plans and Payers
  - Laboratories, Blood and Pharmaceuticals
  - Mass Fatality Management Services
  - Medical Materials
- Security vendors, consultants and service providers not specifically identified as critical healthcare infrastructure, or otherwise not uniquely essential to the support of healthcare service delivery, may contribute in an advisory capacity as requested by the membership, but not as voting members

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

How is the HSCC Different from a Trade Association?

- The HSCC is an *association of associations and their members*, with one unified focus: coordinated critical infrastructure protection (CIP) – both cyber and physical, working toward the common good
- As a recognized partner with the government under presidential executive orders (PPD 21 as amended), the HSCC-HHS ongoing partnership is given special protection from Freedom of Information Act exposure, per below
- To encourage and protect exchange of sensitive CIP information and planning, all SCC's – *not individual trade associations* – when collaborating with government are designated as "CIPACs" – Critical Infrastructure Protection Advisory Committees
- In order to maintain its CIPAC status, an SCC cannot directly lobby the way an association or company can
- **The SCC does not / cannot charge dues in order to retain its FOIA-exempt status when collaborating with government (dues are considered exclusionary)**

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

Why Participate in the HSCC?

- Collectively develop policy and operational solutions to shared challenges facing the security & resiliency of individual enterprises and the sector as a whole
- Build relationships and engage regularly with senior government officials in a trusted environment outside of – and protected from - any regulatory, public disclosure or competitive risks
- Gain visibility into other associations' CIP initiatives in order to deconflict and coordinate for efficient resource management and effectiveness
- Contribute to unity of effort as counter-balance against regulatory or legislative intervention
- Demonstrate thought leadership toward the common good
- Step up to your organization's responsibility for the nation's public health and safety

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

What is the HSCC Cybersecurity Working Group?

- One of the standing Working Groups under the HSCC umbrella
- Tasked with identifying major cybersecurity threats and vulnerabilities to the security and resiliency of the healthcare sector, and developing cross-sector policy and strategic approaches to mitigating those risks
- ~48 healthcare subsector individuals on the roster, many more needed with cross-sector representation

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

How is the HSCC Cybersecurity Working Group Currently Organized?

Current structure:

- Two-Co-Chairs: Terence Rice, Merck; Bryan Cline, HITRUST
- Six task groups (at different stages of progress, to be reassessed):
  - Future Gazing
  - Information Sharing
  - Risk Assessment
  - Risk Management
  - Communications and Marketing
  - 405(d) Implementation (Section 405d of 2015 Cybersecurity Act, requiring HHS to work with industry on cyber security standards of practice)

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

How Will the HSCC Cybersecurity WG Organization Evolve?

Proposed structure:

- Two-Co-Chairs
- Executive Committee comprising one from each of the six healthcare subsectors
- Task Groups focusing on specific deliverables to include:
  - Current workstreams in progress as appropriate
  - Prioritized implementation of Healthcare Cybersecurity Task Force recommendations
  - Medical Device Health IT Joint Strategic Plan
  - Others by consensus
- General membership of HSCC Cyber WG to include any and all association and organizational members with decision making authority, representing critical health subsectors, bringing technical, operational, management and public policy expertise to the table

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

What Executive Roles are Required for Participation?

The Cybersecurity Working Group is composed of senior executives with decision-making authority from industry associations, healthcare enterprises and providers who have technical or managerial responsibility for:

- Cyber risk management
- Information and data management
- Information technology (IT) and operational technology (OT)
- Patient safety
- Product security
- Privacy and security compliance
- Policy, regulatory and legal affairs

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

What is Ahead for the HSCC Cybersecurity Working Group?

- Expand membership from all six subsectors and essential industry associations
- New focus on prioritizing and implementing Healthcare Industry Cyber Security Task Force recommendations compiled under 6 Imperatives:
  1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
  2. Increase the security and resilience of medical devices and health IT
  3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
  4. Increase healthcare industry readiness through improved cybersecurity awareness and education
  5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure
  6. Improve information sharing of industry threats, risks, and mitigations

Healthcare Sector Coordinating Council Cybersecurity Subcommittee Proposed Structure